Office of Inspector General
Corporation for National and Community Service

FEDERAL INFORMATION SYSTEM MANAGEMENT ACT (FISMA) REVIEW OF FY 2005 FOR THE CORPORATION FOR NATIONAL AND COMMUNITY SERVICE

OIG REPORT NUMBER 06-06

Corporation for NATIONAL & COMMUNITY SERVICE

Prepared by:

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

This report was issued to Corporation management on October 14, 2005. Under the laws and regulations governing audit follow-up, the Corporation is to make final management decisions on the report's findings and recommendations no later than April 14, 2006, and complete its corrective actions by October 14, 2006. Consequently, the reported findings do not necessarily represent the final resolution of the issues presented.

Carson

October 14, 2005

Ms. Carol Bates
Acting Inspector General
Office of the Inspector General
Corporation for National and Community Service
1201 New York Avenue NW, Suite 830
Washington, DC 20525

Reference: Contract No. GS-00F-0001N; Task Order No. CNSIG-G-05-002

Subject: Final Report of Independent Evaluation of Corporation for National and Community Service Compliance with the Federal Information Security Management Act for Fiscal Year 2005, OIG Audit Report Number 06-06

Dear Ms. Bates:

The enclosed Independent Evaluation Report is provided in compliance with the above contract. Richard S. Carson & Associates, Inc., on behalf of the Office of Inspector General (OIG) of the Corporation for National and Community Service (CNCS), completed an independent evaluation of the CNCS information security program and posture. This Independent Evaluation Report provides conclusions and findings, identifies problem areas, where applicable, and makes recommendations. Compliance with the E-Government Act of 2002 (Pub. L. No. 107-347) and other Federal guidelines serves as the basis for formulating conclusions, findings and recommendations.

If you have any questions regarding the enclosed document, please contact Diane Reilly at (301) 841-0094 or via e-mail at reilly@carsoninc.com.

Sincerely,

Diane C. Reilly

Diane C. Reilly
Vice President
Information Technology Services

Enclosure

RICHARD S. CARSON & ASSOCIATES, INC.
www.carsoninc.com
4720 Montgomery Lane • Suite 800 • Bethesda, MD 20814-3444 • 301.656.4565 •
Fax: 301.656.4806

[Page intentionally left blank]

BACKGROUND

Richard S. Carson & Associates, Inc. (Carson), on behalf of the Office of Inspector General (OIG), Corporation for National and Community Service (Corporation), has completed an independent evaluation of the Corporation's information security program and posture. This Independent Evaluation Report provides conclusions and findings, identifies problem areas, and where applicable makes recommendations. Compliance with the E-Government Act of 2002 (Pub. L. No. 107-347) and other Federal guidelines serve as the basis for formulating our conclusions, findings, and recommendations.

The E-Government Act of 2002 (Pub. L. No. 107-347), which includes Title III, the Federal Information Security Management Act of 2002 (FISMA), was enacted to strengthen the security of Federal Government information and information systems. FISMA outlines information security compliance criteria for agencies, including the requirement for annual review and independent assessment by agency inspectors general (IGs). These assessments provide agencies with information needed to determine information security effectiveness and to establish strategies and best practices for improving security.

This independent evaluation addresses the Corporation's:

- Information security program.
- Progress towards correcting weaknesses addressed in prior FISMA reports and attendant Plans of Action and Milestones (POA&Ms).
- Review of self-assessments.
- Verification and testing of security controls of information systems.

PURPOSE

The objectives of the independent evaluation were to:

- Determine the efficiency and effectiveness of the Corporation's information security policies, procedures, and practices.
- Test and verify network/system security of a representative subset of the Corporation's major applications (MAs) and general support system (GSS).
- 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) 2004 POA&M.

RESULTS IN BRIEF

The Corporation has taken steps to enhance its security program and address issues identified in the 2004 FISMA report including:

- Periodic network scans to identify vulnerabilities.
- An effective security incident reporting process that follows United States-Computer Emergency Readiness Team (US-CERT) policies.

Several areas of concern noted in the 2004 FISMA report showed little progress toward remediation and/or did not adhere to Office of Management and Budget (OMB) A-130 guidance. The following findings were considered significant deficiencies.

- The Corporation has not complied with Memorandum 03-18, *Implementation Guidance for the E-Government Act of 2002 (Public Law 107-347, 44 United States Code (U.S.C.) Chapter 36),* by not performing a Privacy Impact Assessment (PIA) and reporting the results to OMB.

- The Corporation's security self-assessments do not follow guidance in NIST SP 800-26, *Self-Assessment Guide for Information Technology Systems.*

  1. The documentation to support the reported levels (levels 1-5) is not presently available.
  2. E-SPAN security self-assessment is not finalized and approved; though, the certification and accreditation (C&A) package has been ready since December 2004.

- The Corporation's certification and accreditation efforts are not compliance with the NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems.*

Complete assessment results are presented in the Independent Evaluation section of this report. It details conclusions and findings associated with the review of risk assessments (RAs), security policies and procedures, system security plans (SSPs), security awareness and training, annual testing and evaluation, corrective actions, security incident reporting, continuity of operations (COOP), and configuration management (CM). Major conclusions and findings from the report are summarized in the Results in Brief.

RECOMMENDATIONS

Overall, this independent evaluation resulted in 30 findings and 36 recommendations requiring corrective action. The consolidated list of these recommendations is on page 21.

AGENCY COMMENTS

At the exit conference held on September 14, 2005, Corporation officials generally agreed with the findings. On September 29, 2005, the Corporation provided its response which is included as Appendix C.

The response provided by the Corporation agrees with the three significant deficiencies rendered in the areas of certification and accreditation, privacy impact assessments, and annual security self-assessments. The Corporation has developed a corrective action plan to correct these three significant deficiencies and the remaining deficiencies by March 1, 2006.

ABBREVIATIONS AND ACRONYMS

ATO	Authorization to Operate
C&A	Certification and Accreditation
CASE	Computer-Aided Software Engineering
CCB	Configuration Control Board
CFO	Chief Financial Officer
CIO	Chief Information Officer
CM	Configuration Management
COOP	Continuity of Operations Plan
Corporation	Corporation for National and Community Service
COTS	Commercial Off-the-Shelf
CP	Contingency Plan
CSP	Credential Service Providers
DOI	Department of Interior
DRP	Disaster Recovery Plan
DRS	Disaster Recovery Site
e-Grants	Electronic-Grants
E-SPAN	Electronic-System for Program Agreements and National Service Participants
FPS	Federal Protection Service
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act
FSG	Financial Services Group
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
GAO	Government Accountability Office
GSS	General Support System
HSPD	Homeland Security Presidential Directive
IG	Inspector General
ISACA	Information Systems Audit & Control Association
ISSO	Information Systems Security Officer
IRM	Information Resource Management
IT	Information Technology
LAN	Local Area Network
MA	Major Application
MPD	Washington Metropolitan Police Department
NBC	National Business Center
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OIT	Office of Information Technology

OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
POA&M	Plan of Action and Milestones
RA	Risk Assessment
SDLC	System Development Life Cycle
SIR	Security Incident Report
SMS	Salary Management System
SP	Special Publication
SSP	System Security Plan
ST&E	System Test and Evaluation
U.S.C.	United States Code
UPI	Unique Project Identifier
US-CERT	United States Computer Emergency Readiness Team
VoIP	Voice over Internet Protocol
WBRS	Web-Based Reporting System

TABLE OF CONTENTS

[Page intentionally left blank]

BACKGROUND

Richard S. Carson & Associates, Inc. (Carson), on behalf of the Office of Inspector General (OIG), of the Corporation for National and Community Service (Corporation), has completed an independent evaluation of the Corporation's information security program and posture. This Independent Evaluation Report provides conclusions and findings, identifies problem areas, and where applicable makes recommendations. Compliance with the E-Government Act of 2002 (Pub. L. No. 107-347) and other Federal guidelines serve as the basis for formulating our conclusions, findings, and recommendations.

The E-Government Act of 2002 (Pub. L. No. 107-347), which includes Title III, the Federal Information Security Management Act of 2002 (FISMA), was enacted to strengthen the security of Federal Government information and information systems. FISMA outlines information security compliance criteria for agencies, including the requirement for annual review and independent assessment by agency inspectors general (IGs). These assessments provide agencies with information needed to determine information security effectiveness and to establish strategies and best practices for improving security.

This independent evaluation addresses the Corporation's:

- Information security program.
- Progress towards correcting weaknesses addressed in prior FISMA reports and attendant Plans of Action and Milestones (POA&Ms).
- Review of self-assessments.
- Verification and testing of security controls of information systems.

PURPOSE

The objectives of the independent evaluation were to:

- Determine the efficiency and effectiveness of the Corporation's information security policies, procedures, and practices.
- Test and verify network/system security of a representative subset of the Corporation's major applications (MAs) and general support system (GSS).
- 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) 2004 POA&M.

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 standards 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). When appropriate, root cause and effect are included in the discussion. Recommendations corresponding to these conclusions and findings are intended to assist the Corporation in determining the action needed to correct identified weaknesses and/or deficiencies.

Agency Risk Assessments

Conclusions and Findings

Risk assessments (RAs) were not performed in a timely manner. The Corporation's network underwent a significant change[1] that requires a recertification to continue to be authorized to operate (ATO). OMB A-130 requires that every information system undergo C&A at least every three years, or when a significant change takes place. As part of the C&A process, a RA is performed to determine any vulnerabilities or risks that could be mitigated to an acceptable level. This requirement is for stand-alone systems as well. The Corporation did not perform RAs associated with the migration of operating systems to determine the level of risks associated with installing a new operating system in their environment. Additionally, the Corporation connected Voice over Internet Protocol (VoIP) servers to the general support system (GSS) without performing a RA to determine the vulnerabilities associated with these appliances. This left open potential vulnerabilities and threats of internal or external unauthorized use. By not performing RAs in a timely manner, the inter-connected systems cannot be informed of changes that could affect the security posture in which those systems inter-connect. In addition, by not performing a RA when a significant change occurred, senior management cannot ensure the security posture of the Corporation's information systems.

The Corporation has not conducted a RA on the Employee Badge System prior to going operational. The Badge System is an operational system that was placed into production without a formal RA. Implementing systems, whether they stand-alone or connect to the Corporation's GSS, without performing a RA leaves the Corporation vulnerable to internal and external threats. These threats can be mitigated to an acceptable level should these systems be properly maintained and brought into compliance with Federal mandates, guidance, and best practices of the security industry.

In addition, by not performing a RA when an addition to the Corporation's infrastructure is implemented, senior management cannot ensure the security posture of the Corporation. Undocumented systems are potential entry points for would-be hackers.

The RA process has not been integrated into a formalized C&A process. This is a repeat finding from the FISMA FY 2004 review. The following condition was reported:

> OMB A-130 states that Federal agencies include a risk assessment in the C&A process. NIST Special Publication (SP) 800-18, *NIST Guide for Developing Security Plans,* provides guidance on how to develop a RA.

Risk Assessments do not always follow NIST guidance. The RAs for the Corporation's MAs and GSS follow NIST SP 800-18 with one omission. Section II, Risk Assessment Approach, does not indicate the names of participants involved in developing the RAs. The soundness of the RAs rests on the level of authoritative knowledge of the participants. Not identifying the participants puts the RAs in question in terms of validity and creditability.

The Corporation Office of Information Technology's (OIT) position on the finding that the RAs are not in compliance with the NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, in

[1] Examples of significant changes to an information system that should be reviewed for possible reaccreditation include but are not limited to: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications to system ports, protocols, or services; (iii) installation of a new or upgraded hardware platform or firmware component; or (iv) modifications to cryptographic modules or services. Changes in laws, directives, policies, or regulations, while not always directly related to the information system, can also potentially affect the security of the system and trigger a reaccreditation action.

that, "... this guidance and is not binding (see section 1.1 Authority) ." However, the Corporation has not recognized the position detailed in OMB Memoranda 04-25 and 05-15, which state respectively:

- Memorandum 04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*, page 5, states, "Is use of NIST publications required? Yes, for non-national security programs and systems, agencies must follow NIST standards and guidance. Federal Information Processing Standards (FIPS) must be implemented as written; the only flexibility exists within the standard itself. Special publications of the NIST 800 series and other NIST publications are guidance. As a general rule, use of NIST guidance is more flexible, provided agency implementation is consistent with the principles and processes outlined within the NIST guidance. However, from time to time, OMB policy will mandate stricter use of NIST guidance. For example, NIST SP 800-26 is mandatory for use for agency annual systems reviews. Reviews and evaluations of agency IT security programs and systems should consider adherence to standards and consistency with NIST guidance. Where flexibility exists, evaluations must consider unique operational environments and allow for a reasonable degree of discretion."

- In Memorandum 05-15, *FY 2005 Instructions for Preparing the Federal Information Security Management Act Report and Privacy Management Report*, it states, "Is use of National Institute of Science and Technology (NIST) publications required? Yes. For non-national security programs and systems, agencies must follow NIST standards and guidance."

Recommendations

We recommend that the Corporation:

- Conduct RAs to ensure the Corporation's MAs and GSS are in compliance with Federal mandates and guidelines.

- Perform RAs on all newly acquired systems.

- Integrate the RA process into a formalized C&A process.

- Add a list of participants to Section II, Risk Assessment Approach, for each RA.

Security Policies and Procedures

Conclusions and Findings

The Corporation has made an effort to comply with Development of Homeland Security Presidential Directive M-05-24 (HSPD)-12, *Policy for a Common Identification Standard for Federal Employees and Contractors.* Homeland Security Presidential Directive 12 (HSPD-12) was issued by the White House on August 27, 2004 and updated May 16, 2005. HSPD-12 requires Federal departments and agencies to have, by June 27, 2005, a program in place to ensure identification issued to Federal employees and contractors meets a common standard. Government Corporations are encouraged but not required to implement this directive. The Corporation, in its attempt to comply with the reporting requirements outlined in M-05-24, purchased a Badge System, which is currently in production at the Corporation. However, the Corporation's premature implementation of the Badge System to be in compliance and to meet HSPD-12 requirements, has not fully been integrated. For instance, the Corporation does not require and in some cases does not hold an up-to-date background investigation on key Corporation personnel in sensitive positions.

The Corporation has a library of current policies and procedures. The library of policies and procedures is available to the Corporation through intranet access and includes guidelines for obtaining accounts to the network, using Internet and e-mail systems, protecting sensitive information, and responding to incidents. Subject areas cover both network system and agency-wide security topics. Roles and responsibilities are defined for applicable staff members and contractors when responding to a system failure. This library of policies and procedures gives employees a quick and easy reference for handling security matters.

The Corporation's policy on handling sensitive information is not in compliance with the Corporation's Network System Security Plan (SSP). As a result, the Corporation as a whole is not in compliance with its stated policies. The Network System Security Plan places stricter guidelines on the handling of sensitive information than that included in Policy #501, which informs personnel on how to handle sensitive information. **This is a repeat finding and recommendation from the FISMA FY 2004 review.**

Policy #501, Safeguarding Sensitive Information and Documents, provides a set of standards to be used throughout the Corporation. However, the Corporation's Network System Security Plan places stricter requirements for handling sensitive information. The Corporation's Network SSP, section 1.9, Sensitivity of Information Handled, pages 12 and 13, states:

> The Corporation's Network processes and transmits Sensitive But Unclassified (SBU) data, which requires security services that ensure confidentiality, availability, and integrity of the information processed. There are several applications on the Corporation's Network that process financial information, such as payroll, procurement, stipends, and other commitment of funds or grant payment information. There is also Privacy Act information that the Network transmits and stores on file servers within the Network boundary.

In addition, the Network SSP, section 3.3, *Production Input and Output Controls*, page 22, states:

> In Place Controls: The OIT Help Desk is available to all users for support with system problems, questions, or concerns. Appropriate controls are implemented when handling sensitive information such as signed receipts, registered mail, and locked or monitored client "boxes." *All printouts and electronic data containing sensitive information are clearly labeled to prevent accidental release and inadvertent disclosure of sensitive*

information. The Corporation has published a separate policy regarding safeguarding sensitive information and documents. (Emphasis reviewers)

The Corporation's Structured Systems Development Life-Cycle (SDLC) Methodology needs improvement. This is a repeat finding from the FISMA FY 2004 Review. As part of the FISMA FY 2005 review the current and draft versions of the SDLC were reviewed and several items were found lacking. The items lacking from the current Corporation Policy #378, *Structured Systems Development Life-Cycle Methodology,* are:

- Identification of security personnel.
- Definition of roles and responsibilities.
- Identification of disposal phase and procedures.
- Proper Identification of security controls.

Additionally, the SDLC does not have mechanisms in place, nor proper documentation, to handle:

- **Information Preservation**: Ensures that information is retained, as necessary, to conform to current legal requirements and to accommodate future technology changes that may render the retrieval method obsolete.
- **Media Sanitization:** Ensures that data is deleted, erased, and written over as necessary.
- **Hardware and Software Disposal**: Ensures that hardware and software is disposed of as directed by the information system security officer (ISSO).

For example, the draft SDLC does not include a methodology to dispose of hardware or software. NIST SP 800-64 outlines five distinct SDLC phases: Initiation, Acquisition/Development, Implementation, Operation/Maintenance, and Disposition. The Corporation includes the first four phases in its SDLC, but does not address a disposal procedure.

Additionally, the current SDLC does not contain a methodology for evaluating and integrating Commercial-Off-the-Shelf (COTS) products into the Corporation's automated systems. OMB A-130 and NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle,* calls for establishment of security measures throughout the life cycle. Many agency systems contain pre-packaged products that can offer advanced capabilities without extensive customization by the technical staff. However, while these capabilities are not developed by the agency, the products are integrated into the collective architecture and can have a major impact upon security configurations and practices. Therefore, COTS products should be addressed in the agency's SDLC documentation.

The Corporation's Rules of Behavior (ROB) do not adequately reflect other Major Applications' (MAs) ROB where applicable. The Corporation's ROB does not discuss specific items from the Momentum ROB, *Appendix F,* page F-3, *III, Momentum Application Rules*, such as:

> *Momentum data will be treated as sensitive. Users will not use information contained in Momentum for unauthorized purposes. Momentum contains sensitive financial data that could cause damage to an individual or organization through unauthorized disclosure.*

By not adequately informing users of the potential for additional requirements that may be imposed by additional systems' rules of behavior, the Corporation is accepting risks that were mitigated by placing the major application's ROB into place. The major application's ROB are system-specific and should follow NIST and OMB guidance.

The Corporation has not formally documented its C&A policy. This is a repeat finding, for the third year. FISMA requires "not less than annual" testing and evaluation of the effectiveness of information security policies, procedures, and practices to ensure that system environments remain secure [Section 3544(b)(5)]. NIST SP 800-26, *Self-Assessment Guide for Information Technology Systems*, suggests annual self-assessments be performed to satisfy the requirement for annual testing and evaluation. However, the Corporation has opted to establish an annual C&A process in lieu of annual self-assessments. This was the stated practice at the time of the FY 2003 FISMA independent audit, which generated the recommendation that the practice be documented. The practice has not yet been established in writing, and the potential adverse effect of not performing annual testing and evaluation remains a valid concern.

Recommendations

We recommend that the Corporation:

Develop and implement policies and procedures for the Badge System to meet HSPD-12 compliance.

- Maintain an online library with up-to-date information that is reviewed for clarity and compliance with Corporation, OMB, NIST, and Federal mandates and guidelines.

- Update the Corporation's Policy #501 to reflect the current requirements of the Corporation's Network SSP.

- Update and formally approve Policy #378, *Structured Systems Development Life-Cycle Methodology,* by second quarter FY 2006, in accordance with NIST SP 800-64. Areas noted to be addressed are:

    1. Identification of security personnel.
    2. Definition of roles and responsibilities.
    3. Identification of disposal phase and procedures.
    4. Proper identification of security controls.

- Update the Corporation's ROB to adequately address requirements of the MAs and GSS.

- Document and enforce the stated practice of annual C&As every 12 months to meet the FISMA requirement for testing and evaluation.

- Provide Corporation personnel the major application's ROB and with information on the consequences of non-compliance with the ROB.

System Security Plans

Conclusions and Findings

The Corporation's System Security Plans (SSPs) do not always follow NIST and OMB guidance. In this year's FISMA review, three of seven SSPs were reviewed. Although the Corporation's SSPs present current and planned controls for ensuring protection of the Corporation's GSS and MAs, several areas for improvement were noted during the review of the SSPs.

The SSPs do not include a list of previously conducted security control reviews. This is a repeat finding from the 2004 FISMA report. NIST SP 800-18 provides guidance on how to "describe the type of review and findings conducted on the general support system or major application in the last three

years" and to "include information about the last independent audit or review of the system and who conducted the review" [Section 4.2, Review of Security Controls, page 19]. This methodology and traceability is not present in any of the Corporation's SSPs. Not having the reviews listed and not identifying the persons who conducted the reviews can lead to duplication of effort, waste of resources, and can leave previously identified risks unmitigated. The potential for an unmitigated risk leaves the Corporation vulnerable to internal/external threats.

The Corporation's Network SSP does not specifically address that the MAs are required to follow the Network ROB. The Corporation's Network ROB also does not direct the users of the MAs to review and accept the ROB for the associated applications. OMB A-130 requires that agencies "establish a set of rules concerning the use of and behavior within the application." [Appendix III, A (3)(b)(2)(a)] OMB A-130 also states that:

> Such rules shall clearly delineate responsibilities and expected behavior of all individuals with access to the application. In addition, the rules shall be clear about the consequences of behavior not consistent with the rules.

The Momentum SSP does not consistently identify planned controls. The Momentum SSP is not following NIST SP 800-18, *Security Plan Guide.* It is not identifying the activities that are **planned** for the system in each section of the SSP, where applicable. For example, the SSP states:

> In-Place Controls: Access to the data on the Momentum system is limited to information needed to perform one's duties. Corporation computer security policy provides overall Corporation security policy and provides information on responsibilities with regard to use of the Corporation's automated information systems. The policy document clearly delineates responsibilities and expected behavior of all individuals with access to the GSS on which Momentum resides. Application-specific rules of behavior were documented by the Financial Services Group (FSG) in 2001 and were made available to all users. Although users are currently not required to sign a form acknowledging that they understand their responsibilities toward the protection of Momentum, ***plans are in place to require their signatures.*** (Emphasis reviewers)
>
> While in the Momentum SSP, section 3.1, page 14, it states:
>
> Planned: Individuals occupying positions with a higher level of security designation will be subjected to a full background investigation under procedures being finalized by Human Resources. These procedures will ensure that under no circumstances are these individuals allowed system access prior to completion of background screening.

The Momentum SSP does not identify the location of the Disaster Recovery Site. The Corporation did not properly identify or test the appropriate Disaster Recovery site for Momentum. This finding was recognized during the development of Momentum's SSP and was not adequately addressed in the Momentum's SPP or placed on the Corporation's POA&M for remediation.

The Draft E-SPAN Application Security Plan does not contain system-specific rules of behavior. Rules of behavior were not available for review. Not having these rules can lead to confusion and misunderstanding concerning responsibilities for protecting information. E-SPAN users may be unaware of application-specific data sensitivities and/or be unaware of who is authorized to release grant data through the system, leading to the possible mishandling of information.

A summary of the MA and GSS security plans is not included in the Corporation's Information Technology (IT) Strategic Plan. This is a repeat finding previously cited in the FY 2003 and FY 2004 FISMA reports. OMB A-130 requires that "a summary of the security plans shall be incorporated into the strategic Information Resource Management (IRM) plan required by the Paperwork Reduction Act (44 U.S.C. Chapter 35)" [Appendix III, A (3)(a)(2) and (5)(c)].

Recommendations

We recommend that the Corporation:

- Update all of the Corporation's SSPs in accordance with NIST SP 800-18.
- Update the Corporation's Network SSP to indicate there are additional system-level ROBs to be adhered to, in accordance with OMB and NIST guidance.
- The SSP for Momentum needs to be updated to reflect:

    1. Identification and remediation of planned controls.
    2. Identify location of the Disaster Recovery Site and:

        a. Testing the site.
        b. Maintaining documentation of the testing.
        c. Train the personnel that would be affected by the outcome of the testing.
        d. Implement the recommendations.

- Include SSP summaries in the IT Strategic Plan.

Security Awareness and Training

Conclusions and Findings

The Corporation's Security Awareness Program Needs Improvement. Corporation policy requires all employees and contractors with system access to undergo annual security awareness training. The policy also requires new users to complete security awareness training prior to being authorized access to the Network. OMB A-130 requires that "agencies provide security awareness training for all employees" [2003 FISMA Guidance, page 34]. The Security awareness for this year's effort lacks the ability to adequately train the Corporation's personnel in their responsibilities for security and resources of the Corporation. As a result, the Corporation's security awareness program is not in compliance with OMB guidelines.

Areas for improvement in the Security Awareness Training Program are:

- Program content is insufficient to properly train the Corporation's employees on security best practices, policies, and procedures. For example, the program does not inform users of current information threats and network vulnerabilities facing the Corporation. (i.e., peer-to-peer file sharing, worms, Trojans, etc). Rather, the "training" is limited to employees taking a test. There is no training that precedes the test questions.
- There is no method for tracking an employee's knowledge and if the testing materials have been read and/or understood.

- The Security Awareness Training Test provides no:

    - Tracking mechanism to indicate which users have completed the course
    - Actual training to increase knowledge
    - Tabulation and reporting of an employee's test results in the advent they select a wrong answer,
    - Materials to assist an employee in better understanding their role in security.

- The "test" feature integrated into the security awareness program does not evaluate the knowledge a user should learn from the program.

The "Security Awareness Training Test" administered online to all Corporation employees can be usurped by selecting the alternate choice should the user get an answer wrong. A user can take the test and by-pass the information by selecting the alternate answer and go onto the next question of the series without having read the material. Of the questions asked, some are misleading or inaccurate. Also, there is no tracking mechanism in place for capturing the user's answers and grading them accordingly. There are no additional materials given to the user to gain the knowledge necessary for their responsibilities.

The Information Systems Security Officer (ISSO) maintains a database of all user security awareness testing and proactively prompts users when annual requirements come due. The current database used by the ISSO is manually maintained and tracking is not comprehensive enough to give a clear picture of individual user's knowledge of security practices. Metrics should be incorporated into the current test to capture the user's knowledge on the Corporation's security practices. Some examples of metrics include:

- Ratio of right to wrong answers.
- A percent score that is considered passing.
- How long it took to obtain a passing score.
- Which questions on security awareness are most often answered incorrectly.

Procedures are also in place for training new hires prior to obtaining their accounts and access to major applications and sensitive information. They are required to take the security awareness training test. However, there is no ongoing effort to further assist employees to meet the annual security training requirement.

Recommendations

We recommend that the Corporation:

- Enhance the security awareness training program by incorporating information on current information security threats, network vulnerabilities facing the Corporation, and best practices.

- Enhance the security awareness training program by providing additional training to employees to further develop their knowledge of IT security.

- Develop a comprehensive security awareness training test that adequately addresses:

    1. The content of the security training program.
    2. Possible usurpation by employees.
    3. Tracking the employee's progress throughout the training.
    4. Verifying that the user is aware of security treats and consequences.

Annual Testing and Evaluation

Conclusions and Findings

Annual self-assessments do not comply with NIST guidance. OMB and NIST guidance requires that annual self-assessments be performed annually. OMB Memorandum M-05-15 states:

> At least annually, FISMA (section 3544(b)(5)) 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 evaluation shall include the testing of management, operational, and technical controls.

The Corporation has seven systems but only three systems' self-assessments were available for review, of which one that was in draft. The remaining three systems do not have self-assessments. None of the self-assessments available for review complied with NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems*. Specifically, NIST SP 800-26, Appendix C, page C-4, states:

> Level 1, all written policy should contain the purpose and scope of the policy, the individual(s) responsible for implementing the policy, and the consequences and penalties for not following the policy. The policy for an individual control must be reviewed to ascertain that the criteria for level 1 are met. Assessing the effectiveness of the individual controls, not simply their existence, is key to achieving and maintaining adequate security.

The self-assessment reviewed showed some critical elements were marked at higher levels than control objectives under that category. According to NIST SP 800-26, certain conditions must be implemented before the next level can be achieved. Therefore, the level assigned to the critical element can be no higher than the lowest level assigned to the control objective under that critical element. The levels obtained in the ASSET Tool reports and summaries are inconsistent with the current documentation and infrastructure. In order for a level to be reached, it must meet all of the criteria at the lower level designation. For example, for a control to be marked as a Level 3, then Levels 1 and 2 must be met.

As a result of the self-assessments not being in compliance with NIST SP 800-26, the requirement for annual testing and evaluation has not been met for the Corporation's MAs and GSS. **This is considered a significant deficiency.** FISMA [Section 3544(b)(5)] requires "not less than annual" testing and evaluation of the effectiveness of information security policies, procedures, and practices to ensure that system environments remain secure. FISMA requires annual self-assessments be performed to satisfy the requirement for annual testing and evaluation. The Corporation's stated practice is to perform annual C&As in lieu of self-assessments. Not having *annual testing and evaluation of management, operational, and technical controls* can permit new threats and vulnerabilities to go undetected for an extensive period of time. There is a requirement to ensure that the *management, operational, and technical controls* are performing in the manner in which is expected. In addition to being non-compliant, absence of annual testing and evaluation poses a high risk to the Corporation's information security environment.

The Corporation performs scans of their network to identify vulnerabilities and takes appropriate steps to mitigate risk. OIT staff conducts internal scanning using specialized scanning software. The staff performs detailed vulnerability scans of their architecture to identify such issues as patch update requirements and open ports and services running on various servers, routers, and workstations. These scans are executed routinely. They are also run after a change has been made to the architecture. The OIT methodology includes performing system changes/updates on a test platform and re-running applicable scans to validate changes prior to deployment in the production environment.

Not all vulnerabilities from previous independent reviews have been remediated. Since the FISMA FY 2003 review, there has been, and still exists, a vulnerability which was brought to OIT's attention to further investigate, validate, and remediate. The vulnerability would give a would-be intruder/hacker/disgruntled employee access to the Corporation's privacy information.

Should the privacy information be extracted and abused, it could cause irreparable damage. If this vulnerability were exploited, it could damage the confidentiality and integrity of the Corporation's information systems or lead to serious harm to the reputation and integrity of the Corporation.

Recommendations

We recommend that the Corporation:

- Conduct annual self-assessments in accordance with NIST SP 800-26 or NIST SP 800-53.
- Continue to exploit established internal and external scanning procedures as a means of identifying network vulnerabilities and taking corrective action to mitigate risk.
- Remediate outstanding vulnerabilities identified in previous independent reviews.

Corrective Action Process (Plan of Action and Milestones)

Conclusions and Findings

The Corporation maintains a single, agency-wide POA&M and reports POA&M status to OMB on a quarterly basis as required. The Corporation has instituted changes to the POA&M process in response to the FY 2004 FISMA review. The ISSO, with the assistance of the Deputy Chief Information Officer (CIO) has implemented system-level tracking for each system currently undergoing C&A efforts at the Corporation. As a result, the POA&M now has greater granularity below summary level than were submitted in the past. The refined process allows for OMB compliance by giving the Corporation the ability to track IT security weaknesses identified through audits, assessments, and investigations conducted on the Corporation. However, the Corporation is not following OMB guidance with regard to properly maintaining the POA&M for the OMB quarterly submission.

The Corporation's POA&M does not comply with OMB Guidance. OMB Guidance, Memorandum M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*, page 15, states that the heading of each POA&M must include the unique project identifier from the Exhibits 300 and 53, where applicable.[2] The OMB guidance also states, once an agency has completed the initial POA&M, no changes should be made to the data in columns 1, 4, 5, and 7.

Our review of the FY 2005 POA&M showed:

- It does not have a Unique Project Identifier (UPI) for each system being tracked. The Corporation has not placed the UPI on the POA&M that is submitted quarterly to OMB.

[2] OMB Circular A-11 requires that agencies develop and submit to OMB capital asset plans (Exhibit 300) for major acquisition projects. For information technology projects, plans for major systems must be reported to OMB on an Exhibit 300 and 53. The agency assigns a unique identifier to each system and applies it to both exhibits.

- There were changes made to the columns specified by OMB that should not be changed once a POA&M has been submitted. For example, on the second quarter FY 2005 POA&M submitted to OMB, items have been removed prior to one year after closure of an item has elapsed.

Additionally, the Corporation has submitted the second quarter FY 2005 update to the OMB with line items removed from the Corporation's first quarter FY 2005 update.

By not complying with OMB guidance, OMB will not be able to accurately track IT issues facing the Corporation.

The POA&M does not capture all weaknesses reported. It is not capturing all of the weaknesses reported in the audits, system reviews, and assessments conducted on the Corporation and applying them to the POA&M process for proper oversight and resolution. Here are some examples:

- The Corporation's Network Risk Assessment, dated February 22, 2005, and signed by the Designated Approving Authority (DAA) on July 6, 2005, identifies risks, with their associated recommendations, that are not on the POA&M submitted to OMB for the second quarter dated March 15, 2005. The information is also missing from the third quarter POA&M submission, dated June 15, 2005.

- The Corporation's Momentum Risk Assessment dated February 18, 2005, identifies risks, with their associated recommendations, which are not on the POA&M submitted to OMB for the second quarter dated March 15, 2005, nor are they on the third quarter POA&M submission, dated June 15, 2005.

- The Corporation did not capture some of the weaknesses on the POA&M identified in the Momentum C&A package including:

  1. Slow processing time.
  2. System owner is not involved in upgrade/security decisions.

- The Momentum Disaster Recovery Plan (DRP) report identified several weaknesses and significant security concerns that were not tracked in the POA&M. These weaknesses are:

  1. No provisions for contacting the Corporation in the event of a disaster.

  2. The detailed instructions for recovering the Momentum application are not included.

  3. There is no guidance provided on network connections for the Corporation to the SunGard facility. SunGard has been designated and contracted to be the Disaster Recovery site for personnel in the event the Corporation has declared a disaster. SunGard is located in Herndon, VA with multiple alternate sites within the area. Coupled with the lack of provisions for contacting the Corporation, this could significantly increase any downtime if SunGard should move the recovery of Momentum from its local Metro Center to some other location.

By not capturing all the weaknesses, the Corporation is not in compliance with OMB directives, and senior management cannot be sure of the current security posture of the Corporation's resources and assets.

Recommendations

We recommend that the Corporation:

Improve the current single, agency-wide POA&M process:

- Develop and implement policies and procedures for ensuring that all items noted as weaknesses or findings in the various audits, reviews, and investigations are captured and remediation included on the official POA&M.

- Maintain the POA&M's structure and information in accordance with OMB Guidance, to address:

    1. The tracking of all weaknesses to closure.
    2. Retaining all weaknesses tracked to ensure that items, once placed on the official POA&M, are not removed until one full year after the quarter in which those items are closed.

Security Incident Reporting

Conclusions and Findings

The Corporation has developed and maintains an effective security incident reporting process [effective March 2004 US-CERT]. OMB A-130 requires that all agencies develop an incident-response capability for their MAs and GSSs [2003 FISMA, page 35]. The Corporation developed and maintains a detailed policy that follows the United States-Computer Emergency Readiness Team (US-CERT) policies. The policy is available to all users through the Corporation's intranet, providing thorough guidance concerning security incident report (SIR) procedures and responsibilities. The Deputy CIO and ISSO take an active role in the SIR process, particularly for IT-related incident reporting. The Deputy CIO is very knowledgeable regarding what types of incidents are considered "reportable" and the procedures to be used to invoke the reporting process. In the past year no incidents at the Corporation's headquarters, its Service Centers, or State Offices have required an SIR. A responsibility of Administrative Services, notification procedures provide for immediate reporting if a physical security incident occurs. If the incident takes place within the headquarters facility, Administrative Services contacts the Federal Protective Services (FPS), which, in turn, responds. The Washington Metropolitan Police Department is contacted for response to incidents outside the headquarters facility.

Continuity of Operations and Disaster Recovery

Conclusions and Findings

The Corporation does not have an approved and documented Continuity of Operations Plan (COOP) or system-level contingency plans (CPs) as required by NIST, OMB, and Federal guidelines. In Federal Preparedness Circular (FPC) 65, dated June 15, 2004, it states:

> Policy: It is the policy of the United States to have in place a comprehensive and effective program to ensure continuity of essential Federal functions under all circumstances. To support this policy the Federal Executive Branch has implemented the COOP Program. COOP is defined as the activities of individual departments and agencies and their sub-components to ensure that their essential functions are performed. This includes plans and procedures that delineate essential functions; specify succession to office and the emergency delegation of authority; provide for the

> safekeeping of vital records and databases; identify alternate operating facilities; provide for interoperable communications; and validate the capability through tests, training, and exercises. All Federal agencies, regardless of location, shall have in place a viable COOP capability to ensure continued performance of essential functions from alternate operating sites during any emergency or situation that may disrupt normal operations.

By not having a COOP, the Corporation is not in compliance with OMB requirements. The absence of an approved COOP leaves the Corporation open to vulnerabilities that could have been uncovered, and also without plans put in place to mediate the risks associated with those vulnerabilities. Additionally, the Corporation is unable to test, train, and prepare staff.

NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems,* states that contingency plans should contain detailed records of system configurations in order to enhance system recovery capabilities. In the Executive Summary of NIST SP 800-34, it states:

> Accordingly, in order for contingency planning to be successful, agency management must ensure the following:
>
> - Understand the IT contingency planning process and its place within the overall COOP and Business Continuity Plan process.
> - Develop or reexamine their contingency policy and planning process and apply the elements of the planning cycle including preliminary planning, business impact analysis, alternate site selection, and recovery strategies.
> - Develop or reexamine their IT contingency planning policies and plans with emphasis on maintenance, training, and exercising the contingency plan.

The FISMA review found that none of the Corporation's systems have contingency plans. By not having a system level CP, the Corporation is not able to properly test, train, and input a logical progression of events for each system should the need arise. There are a myriad of issues that are raised and uncovered during the annual testing of each plan. Some of the more common ones are:

- Roles and responsibilities of each CP member.
- Personnel changes.
- New threats.
- Outdated documentation.
- Inaccurate documentation.

The Corporation has not updated its Disaster Recovery Plan (DRP). This is a repeat finding from the FY 2004 review. The Corporation's DRP generally adheres to NIST SP 800-34 guidelines. However, these discrepancies were noted:

- Disaster recovery team responsibilities are not defined.
- The operating systems in use conflict with the DRP.
- The Corporation's organizational chart has not been implemented into the plan, making it unclear as to which personnel are on the active recovery team.

Not having roles and responsibilities properly defined can make it difficult for the Corporation to effectively execute the DRP in case of a disaster.

The Momentum DRP has not been updated. The Corporation has not been proactive in following the recommendations contained in the Momentum DRP Report dated February 25, 2005. The report provides an evaluation of the existing *Disaster Recovery and Backup Plan – Momentum Environment* and the *NBC Reston LAN GSS Enclave Contingency Plan* maintained by the National Business Center (NBC) for Momentum. Momentum is hosted at NBC, a Department of the Interior organization. Momentum's DRP conforms to FISMA requirements by describing the strategy for recovery.

The Corporation reported the following in the Momentum Security Plan:

> Planned Controls: The disaster recovery plan was originally developed for the Reston, VA, facility. It needs to be updated to reflect the recent relocation of the facility to Ashburn, VA. In addition, a list of critical contact persons is not included in the plan. The Corporation is currently in the process of formulating this list, which will be included in the updated Disaster Recovery Plan.

A limited CP test was conducted in September 2003 which did not test the Alternate Disaster Recovery Site (DRS) and the test results were not documented. The testing in the September 2003 scenario was interrupted by a live recovery operation. No further actions regarding this finding have taken place.

To date, the DRP has not been updated with the "planned" controls described above and test results have not been documented.

Recommendations

We recommend that the Corporation:

- Formally approve and test the COOP, train employees, and document and retain test results for inclusion in future reports, audits, reviews, and independent evaluations.
- Develop Contingency Plans for the facility, MAs, and GSS in accordance with NIST SP 800-34 and OMB guidance.
- Update the Corporation's DRP and Momentum documentation to fully meet NIST 800-34 guidelines.

Configuration Management

Conclusions and Findings

The Corporation has not formally accepted the Configuration Management Process documentation. NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle, Revision 1*, states that "managing and monitoring" are key components of systems configuration. In this regard, the Corporation has implemented many CM activities. All hardware is maintained by an inventory tracking system managed by the OIT. This inventory is reviewed at least once annually as required by FISMA, Section 305. Software licensing and installations are managed by the OIT Client Support Group, with oversight by the Deputy CIO. Automation tools are used by the OIT to maintain system-level configuration and desktop deployments. Additionally, application configurations are controlled through a Configuration Control Board (CCB), with CIO and Deputy CIO involvement in security issues. The CCB recommendations that have budget considerations or decisions have to be approved by the Chief Financial Officer (CFO). The OIT also utilizes Computer-Aided Software Engineering (CASE) tools from Oracle to design, develop, and maintain security settings and database roles/permissions within application databases. To further enhance the CM program, a CM Plan should be developed. This will bring together the many CM activities into a single integrated process, and formalize the CM process for greater "managing and monitoring" benefits.

Recommendations

Based on findings associated with the Corporation's draft Configuration Management Plan, a thorough review of the plan should be undertaken and then be formally accepted by senior management.

Certification and Accreditation (C&A)

Conclusions and Findings

Not all Corporation systems have C&As. This is considered a significant deficiency. As of May 2004, all system C&As have to be in compliance with FIPS 199 and NIST SP 800-37, per OMB Memorandum M-04-25. The Corporation has seven systems that require C&As to be performed, and they include:

- General Support System (Network)
- Momentum
- E-SPAN
- Salary Management System (SMS)
- Badge System
- Voice over IP (VOIP)
- Web Based Reporting System (WBRS)

Of the seven systems owned and operated by the Corporation, there are three systems that have not been categorized against FIPS 199 or certified and accredited (e.g., SMS, Badge System, and VOIP). FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, page 1, states:

> These standards shall apply to: (i) all information within the Federal Government other than that information that has been determined pursuant to Executive Order 12958, as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate

> its classified status; and (ii) all Federal information systems other than those information systems designated as national security systems as defined in 44 United States Code Section 3542(b)(2).

In FIPS 199, section 3, page 1, it states, "This publication establishes security categories for both information[3] and information systems."

Not categorizing these systems can allow them to remain open to vulnerabilities that could be mitigated should the systems undergo a process to protect the data and information contained within these systems. Senior management cannot know for certain if a particular part of the Corporation's assets are at risk for unauthorized access, tampering, or malicious code insertions through a weakness that has not yet been properly assessed for its risks. There is a potential vulnerability or risk of attack present within these systems that may not be properly mitigated to an acceptable level. The adverse effect on individuals may include, but is not limited to, loss of the privacy to which individuals are entitled under law.

In NIST SP 800-37, it states:

> Required by OMB Circular A-130, Appendix III, security accreditation provides a form of quality control and challenges managers and technical staffs at all levels to implement the most effective security controls possible in an information system, given mission requirements, technical constraints, operational constraints, and cost/schedule constraints. By accrediting an information system, an agency official accepts responsibility for the security of the system and is fully *accountable* for any adverse impacts to the agency if a breach of security occurs. Thus, responsibility and accountability are core principles that characterize security accreditation.

Additionally, the Corporation has not officially authorized E-SPAN to operate. The E-SPAN C&A has been in draft since February 2005 and, as such, was deemed to be out of compliance with OMB and NIST guidance. As a result of C&As not being performed on systems, senior management is not assured of the security posture within the Corporation; leaving the authorizing officials of these systems held accountable for the security threat that these systems impose on the Corporation's resources. The exposure of risks within the C&A process are not being elevated to the POA&M for remediation, leaving those vulnerabilities and threats open to unauthorized persons.

System C&As do not always follow NIST guidance. As part of the FY 2005 FISMA review, two of the seven system C&A packages were reviewed to include Momentum and the Corporation's Network. During the review of the C&A packages, several weaknesses were found. These weaknesses are discussed below.

The Corporation did not follow the C&A process outlined in NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems,* for creating the Corporation's Certification Letter and Accreditation Statements. The C&A letters did not follow the line of succession prescribed in the guidance for informing stakeholders of decisions made in the C&A process.

The Corporation's policy of assigning the individual at the time of granting a full ATO is not in compliance with NIST guidance. As each individual portion of the C&A package is produced, each should be sent to the appropriate officials to be reviewed and for a decision made as to the security

[3] Information is categorized according to its *information type.* An information type is a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, Executive Order, directive, policy, or regulation.

posture that document exposes. The individual documentation generally has items that need to be placed on the POA&M for timely disposition. As it stands, the Corporation has weaknesses that are left unattended until the decision of the Designated Approving Authority (DAA) grants an ATO. However, this leaves the Corporation vulnerable to the weaknesses reported in the various documents used to grant an ATO.

The Corporation has not conducted system testing and evaluation (ST&E) in accordance with OMB, NIST SP 800-37, and NIST SP 800-30 guidance. ST&Es are designed to test the effectiveness and efficiency of the security controls of an IT system as they have been applied in an operational environment, considering impact on the mission. The objective is to ensure that the applied controls meet the approved security specification for the software and hardware and implement the organization's security policy or meet industry standards. By not having conducted ST&E, the Corporation is not fully informed of the risks associated with their systems.

The Corporation does not always perform reaccreditations when a significant change to a system occurs. NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, page 5, states:

> "reaccreditation occurs periodically in accordance with Federal or agency policy and whenever there is a significant change to the system or its operational environment.[4]"

The Corporation did not perform a C&A upon the Network when new systems, including an upgraded network operating system, or services were added. It was noted during the review that the Corporation's network operating system was upgraded without a recertification of the network. Not having systems certified and accredited can result in:

- Non-compliance with NIST and OMB.
- System vulnerabilities are not remediated to an acceptable level.
- Stakeholders within the system boundaries cannot be assured of the security of their system.
- DAAs are held accountable for vulnerabilities that are not remediated to an acceptable level.

Recommendations

We recommend that the Corporation:

- Provide the appropriate line of succession for system notification within the C&A letters.
- Grant the appropriate ATO for E-SPAN to be in production.
- Provide documentation that the C&A is in compliance with OMB and NIST.
- Notify all stakeholders of any significant change to the Corporation's security posture due to a significant change or addition of hardware or software that requires new C&A efforts.

[4] Examples of significant changes to an information system that should be reviewed for possible reaccreditation include but are not limited to: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications to system ports, protocols, or services; (iii) installation of a new or upgraded hardware platform or firmware component; or (iv) modifications to cryptographic modules or services. Changes in laws, directives, policies, or regulations, while not always directly related to the information system, can also potentially affect the security of the system and trigger a reaccreditation action.

- Conduct the activities necessary to bring all systems within the Corporation's operational boundaries in compliance with FIPS 199 and NIST SP 800-37. Perform the following activities (this is not an all-inclusive list):

    1. Policies and Procedures development and publication
    2. Budget Impact Analysis
    3. Risk Assessment
    4. System Security Plan
    5. Security Test and Evaluation (ST&E)
    6. Rules of Behavior
    7. Contingency Plan (updating the appropriate CP for the Corporation's Network)
    8. Configuration Management baselines
    9. Review and grant an ATO, IATO, or Not Authorized to Operate in a timely manner

Privacy

Conclusions and Findings

The Corporation has not complied with Memorandum 03-18, *Implementation Guidance for the E-Government Act of 2002 (Public Law 107-347, 44 U.S.C. Chapter 36).* The Corporation has not performed a Privacy Impact Assessment (PIA) and reported results to OMB. **This is considered a significant deficiency**. The E-Government Act, Section 208, directs agencies to conduct reviews of how personally identifiable information is handled within their agency when collected electronically to ensure this information is accorded proper protection. Agencies are also directed to inform the public of how they handle personal information provided electronically, so that the American public knows their personal information is protected. The Corporation stated in its response to the FY 2004 FISMA Report that the PIA was not required on systems that were already in production. However, the Corporation underwent significant changes in the interim period of reporting, in which PIAs are required. Not being in compliance makes personal information vulnerable to misuse and undermines public confidence in the Corporation's ability to protect personal data it holds.

Additionally, the Corporation has not performed a PIA on any of the newly acquired or operational systems within the Corporation's security boundaries.

The Corporation has not conducted an assessment of its systems for compliance with the E-Authentication Memorandum M-04-04, which implements Section 203 of the E-Government Act, 44 U.S.C. Chapter 36. The Memorandum, Attachment A, Section 1.1, *Introduction Summary,* states:

> This guidance requires agencies to review new and existing electronic transactions to ensure that authentication processes provide the appropriate level of assurance. It establishes and describes four levels of identity assurance for electronic transactions requiring authentication. Assurance levels also provide a basis for assessing Credential Service Providers (CSPs) on behalf of Federal agencies.

The Corporation was mandated to conduct E-Authentication Risk Assessments by the following schedule set by OMB in *Determining Assurance Levels,* Section 5, *Effective Dates of Guidance*:

> Agencies must categorize all existing transactions/systems requiring user authentication into one of the described assurance levels by September 15, 2005. Agencies should accomplish this in the following order:

- Systems classified as "major" must be completed by December 15, 2004.
- New authentication systems should begin to be categorized, as part of the system design, within 90 days of the completion of the final E-Authentication Technical Guidance issued by NIST.

The chosen assurance level must be made publicly available through the agency website, the Federal Register, or other means (e.g., upon request). The E-Authentication Initiative will post agency application assurance levels at a central location for public access.

Recommendations

We recommend that the Corporation:

- Conduct PIAs on all of the systems currently within the Corporation's operational boundaries and under development.
- Conduct a PIA on any new system in development.
- Revisit the PIA for any system undergoing a new C&A effort.
- Conduct E-Authentication assessments for the Corporation's systems to determine compliance with OMB requirements. Make these assessments readily available upon request.

Consolidated List of Recommendations

Agency Risk Assessments (RAs):

1. Conduct RAs to ensure the Corporation's MAs and GSS are in compliance with Federal mandates and guidelines.

2. Perform RAs on the newly acquired systems that are under the auspices of the Corporation's control and purview.

3. Integrate the RA process into a formalize C&A process.

4. Add the list of RA participants to Section II, Risk Assessment Approach, for each RA.

Security Policies and Procedures:

5. Develop and implement policies and procedures for the Badge System to meet HSPD-12 compliance.

6. Maintain an online library with up-to-date information that is reviewed for clarity and compliance with Corporation, OMB, NIST, and Federal mandates and guidelines.

7. Update the Corporation's Policy #501 to reflect the current requirements of the Corporation's Network SSP.

8. Update and formally approve Policy #378, *Structured Systems Development Life-Cycle Methodology,* by second quarter FY 2006, in accordance with NIST SP 800-64. Areas noted to be addressed are:

    - Identification of security personnel.
    - Definition of roles and responsibilities.
    - Identification of disposal phase and procedures.
    - Proper identification of security control.

9. Update the Corporation's ROB to adequately address requirements of the MAs and GSS.

10. Document and enforce the stated practice of annual C&As to meet the FISMA requirement for testing and evaluation every twelve months.

11. Provide the Corporation's personnel the major application's Rules of Behavior and the consequences of non-compliance with ROB.

System Security Plans (SSPs):

12. Update all of the Corporation's SSPs in accordance with NIST SP 800-18.

13. Update the Corporation's Network SSP to indicate there are additional system-level ROB to be adhered to, in accordance with OMB and NIST guidance.

14. The SSP for Momentum needs to be updated to reflect:

- Identification and remediation of planned controls.
- Identification of the location of the Disaster Recovery Site; and

  a) Test the appropriate site.
  b) Maintain documentation of the testing.
  c) Train personnel that would be affected by the outcome of the testing.
  d) Implement the recommendations.

15. Include SSP summaries in the IT Strategic Plan.

Security awareness and training:

16. Enhance the training program by incorporating current information security threats, network vulnerabilities facing the Corporation, and security best practices.

17. Enhance the training program to provide additional security training to employees to further develop their knowledge in IT security,

18. Develop a comprehensive security awareness training test that adequately addresses:

    - The content of the security-training program.
    - Usurpation by employees.
    - The ability to track the employee's progress throughout the training.
    - Verification that the user is aware of the consequences.

Annual testing and evaluation:

19. Conduct annual self-assessments in accordance with NIST SP 800-26 or NIST SP 800-53.

20. Continue to exploit established internal and external scanning procedures as a means of identifying network vulnerabilities and taking corrective action to mitigate risk.

21. Remediate outstanding vulnerabilities from independent reviews.

Corrective action process:

Improve the current single, agency-wide POA&M process:

22. Develop and implement policies and procedures for ensuring that all items noted as weaknesses or findings in the various audits, reviews, and investigations are captured and remediation given on the official POA&M.

23. Maintain the POA&M's structure and information in accordance with OMB Guidance to address:

    - The tracking of all weaknesses to closure.
    - Retaining all weaknesses tracked to ensure that items once placed on the official POA&M are not removed until one full year after the quarter in which those items are closed.

Continuity of operations and contingency plans:

24. Formally accept and test the COOP, train employees, and document and retain test results for inclusion in future reports, audits, reviews, and independent evaluations.

25. Develop Contingency Plans for the facility, major applications, and general support system that are in compliance with NIST SP 800-4 and OMB guidance.

26. Update the Corporation's DRP and Momentum documentation to fully meet NIST 800-34 guidelines.

Configuration Management (CM):

27. Based on findings associated with the Corporation's draft Configuration Management Plan, a thorough review of the plan should be undertaken and then be formally accepted by senior management.

Certification and Accreditation (C&A):

28. Provide the appropriate line of succession for system notification within the C&A letters.

29. Grant the appropriate ATO for E-SPAN to be in production.

30. Provide documentation that the C&A is in compliance with OMB and NIST.

31. Notify all stakeholders of any significant change to the Corporation's security posture due to a significant change or addition of hardware or software that requires new C&A efforts.

32. Conduct activities necessary to bring all systems within the Corporation's operational boundaries in compliance with FIPS 199 and NIST SP 800-37, including: (this is not an all-inclusive list):

    - Policies and Procedures development and publication
    - Budget Impact Analysis
    - Risk Assessment
    - System Security Plan
    - Security Test and Evaluation (ST&E)
    - Rules of Behavior
    - Contingency Plan (updating the appropriate CP for the Corporation's Network)
    - Configuration Management baselines
    - Review and grant an ATO, IATO, or Not Authorized to Operate in a timely manner

Privacy:

33. Conduct Privacy Impact Assessments on all of the systems currently within the Corporation's operational boundaries.

34. Conduct a PIA on any new system in development.

35. Revisit the PIA for any system undergoing a new C&A effort.

36. Conduct E-Authentication assessments for the Corporation's systems to determine compliance with OMB requirements. Make these assessments readily available upon request.

Response to Agency Comments

Carson Associates have reviewed the comments provided, on September 29, 2005, to this report's findings and recommendations. We note from the Corporation's response that they are in agreement with all of the findings and recommendations. We also find, included in their response, that the Corporation has developed a corrective action plan. The Corporation's corrective action plan (CAP) is sufficiently detailed enough to conclude that the Corporation has captured the findings and recommendations addressed in this report. There is sufficient evidence in the Corporation's response to conclude that implementation and closure of the recommendations and findings will be on or about March 1, 2006. Formal review of the Corporation's Plan of Action and Milestones, dated March 15, 2006, should be conducted by or on behalf of the Office of Inspector General to verify the CAP proposed has been accomplished. The formal review would also indicate whether or not reported items are properly handled and tracked to resolution.

OBJECTIVE, SCOPE, AND METHODOLOGY

The overall objective of this independent evaluation was to assist the OIG in meeting its FISMA obligation for independent assessment of the Corporation's information security in accordance with OMB FY 2005 reporting guidelines. In support of this objective, the evaluation team conducted a high-level, qualitative review of the Corporation's information security program, specifically evaluating the agency's degree of compliance with applicable criteria for a security program and evaluating the effectiveness of automated and manual security controls for the four mission-essential systems of the Corporation. Systems examined were:

- Momentum
- E-SPAN (e-Grants as a module of E-SPAN)
- Corporation Network
- FIPS Badge System

These systems were not included in the scope of this audit:

- Web-Based Reporting System (WBRS)
- The OIG Local Area Network (LAN)
- Salary Management System (SMS)
- Contractor-operated facilities.

The scope of work was organized into three tasks:

- Background Review
- Evaluation Fieldwork
- Evaluation Reporting

Consistent with these tasks, the methodology involved data collection (e.g., primarily from interviews and records), data analysis, security controls testing, and determination of findings and recommendations.

Interviews entailed administration of structured question sets (e.g., derived from NIST, the Federal Information Systems Controls Audit Manual and OMB security criteria) to the following Corporation staff:

- Deputy CIO
- CIO
- Program Officials
- Selected OIG staff
- Selected system users

The document review process included agency:

- Plans and policies
- Reports
- Network diagrams
- System certifications and accreditations

An external penetration test was conducted to evaluate security aspects of the agency's firewall. The test was performed from outside the Corporation's security perimeter (e.g., from the Internet). Network vulnerability scans were performed using SAINT® and a variety of penetration testing tools. The results of the external penetration were provided to the Corporation in a separate report.

Analyses were performed in accordance with guidance from the following:

- Government Accountability Office (GAO), *Government Auditing Standards*, 2003 Revision.
- GAO, *Federal Information System Controls Audit Manual*, Volume I: Financial Statement Audits, January 1999.
- NIST Special Publication 800-26, *Self-Assessment Guide for Information Technology Systems*, August 2001.
- OMB reporting instructions.
- Information Systems Audit & Control Association (ISACA) standards.
- Corporation OIG Audit Guidance.

The evaluation was conducted on site at the Corporation headquarters, 1201 New York Avenue NW, Washington, DC 20525, between May 5, 2005, and August 22, 2005. Evaluators were Anthony Van Dyck, Reginald Esteban, and Diane Reilly from Richard S. Carson & Associates, Inc., 4720 Montgomery Lane, Suite 800, Bethesda, MD 20814.

October 7, 2005

The Honorable Joshua B. Bolten
Director, Office of Management and Budget
Eisenhower Executive Office Building
Room 252
Washington, DC 20503

Dear Director Bolten:

The Corporation for National and Community Service (the Corporation) submits for your review its 2005 Federal Information Security Management Act (FISMA) annual report. The Corporation takes its responsibility for ensuring that its information systems and infrastructure are secure and meet FISMA requirements very seriously and is committed to resolving the identified issues and improving our FISMA process.

During the process of conducting this year's FISMA review, the Corporation's Office of the Inspector General (OIG) noted weaknesses in the security posture of the Corporation. The Corporation is implementing a comprehensive plan to correct these weaknesses, this plan is outlined below. In addition, we have contracted with a FISMA consultant to assist in completing these corrective actions by March 1, 2006. Specifically, we will review our systems using the following process.

System Review Process Summary

1. Inventory all Corporation computer systems.

2. Determine if the asset is a significant system. Define all systems into the following:
    a. Major Application (MA);
    b. General Support System (GSS);
    c. Minor Applications (systems that are neither a MA nor a GSS).

3. Categorize all required Systems based on the following:
    a. Identify the level of associated risk by evaluating –
        i. Functionality of the system;
        ii. The types of data the system processes and holds.
    b. Complete Privacy Impact Assessments (PIAs).
    c. Determine whether the system requires an E-Authentication Assessment –
        i. Complete the E-Authentication Assessment when required.

4. For all MAs or GSS:
    a. Develop a controls baseline for the system –
        i. Perform a Risk Assessment for the systems.
    b. Develop a Security Plan for the systems.
    c. Perform an appropriate Security Test & Evaluation ST&E.
    d. Complete an annual Self-Assessment.
    e. Complete the C&As –
        i. Include the necessary documentation to ensure that the C&As are in compliance with OMB and NIST;
        ii. Document the Rules of Behavior (ROB);
        iii. Document the Configuration Management baselines.

The Corporation will complete the inventory and categorization by December 1, 2005 and complete the entire process by March 1, 2006.

Other materials that support this assessment are available for review by your staff. Please contact our Chief Information Officer, Mr. Peter Hill, at 202-606-6609, or via email at phill@cns.gov, should you have any questions regarding the attached information.

Sincerely,

David Eisner
Chief Executive Officer

Enclosure: 2005 FISMA Annual Report

cc: Carol Bates, Acting Inspector General

Section B: Chief Information Officer. Questions 1, 2, 3, and 4.

Agency Name: Corporation for National and Community Service

Question 1 and 2

1. By FIPS 199 risk impact level (high, moderate, low, or not categorized) and by bureau, identify the number of information systems used or operated by your agency, and the n information systems used or operated by a contractor of your agency or other organization on behalf of your agency.

Note: Agency systems shall include information systems used or operated by an agency. Contractor systems shall include information systems used or operated by a contractor agency or other organization on behalf of an agency. The total number of systems shall include both agency systems and contractor systems.

To meet the requirement for conducting a NIST Special Publication 800-26 review, agencies can:
1) Continue to use NIST Special Publication 800-26, or,
2) Conduct a self-assessment against the controls found in NIST Special Publication 800-53

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, therefore, self repo contractors does not meet the requirements of law. Self reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service p have a shared responsibility for FISMA compliance.

FIPS 199, a Federal information processing standard, was published in February 2004. If there are systems which have not yet been categorized, or, if a risk impact level was de through another method, please explain below in item (d.).

2. For each part of this question, identify actual performance in FY 05 by risk impact level and bureau, in the format provided below. From the Total Number of Systems, identi number of systems which have: a current certification and accreditation, a contingency plan tested within the past year, and security controls tested within the past year. Con planning is a requirement for certification and accreditation, with annual contingency plan testing required thereafter. If the number of systems with full certification and accred higher than the number of systems with a tested contingency plan, please explain.

		Question 1						Question 2					
		a. FY 05 Agency Systems		b. FY 05 Contractor Systems		c. FY 05 Total Number of Systems		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and evaluated in the last year		c. Number of systems for which contingency plans have been tested in accordance with policy and guidance	
Bureau Name	FIPS 199 Risk Impact Level	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
Bureau	High	0	0	0	0	0	0	0	#DIV/0!		#DIV/0!		#DIV/0!
CNCS	Moderate	3	3	0	0	3	3	3	100.0%	3	100.0%	3	100.0%
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized	3		1		4	0		0.0%		0.0%		0.0%
	Sub-total	6	3	1	0	7	3	3	42.9%	3	42.9%	3	42.9%
Bureau	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
IG	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	0	0	0	0	0	0	0	#DIV/0!	0	#DIV/0!	0	#DIV/0!
Bureau	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	0	0	0	0	0	0	0	#DIV/0!	0	#DIV/0!	0	#DIV/0!
Bureau	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	0	0	0	0	0	0	0	#DIV/0!	0	#DIV/0!	0	#DIV/0!
Bureau	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	0	0	0	0	0	0	0	#DIV/0!	0	#DIV/0!	0	#DIV/0!
Bureau	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	0	0	0	0	0	0	0	#DIV/0!	0	#DIV/0!	0	#DIV/0!
Bureau	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	0	0	0	0	0	0	0	#DIV/0!	0	#DIV/0!	0	#DIV/0!
Bureau	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	0	0	0	0	0	0	0	#DIV/0!	0	#DIV/0!	0	#DIV/0!

Agency Totals	**High**	0	0	0	0	0	0	0	#DIV/0!	0	#DIV/0!	0	#DIV/0!
	Moderate	3	3	0	0	3	3	3	100.0%	3	100.0%	3	100.0%
	Low	0	0	0	0	0	0	0	#DIV/0!	0	#DIV/0!	0	#DIV/0!
	Not Categorized	3	0	1	0	4	0	1	25.0%	0	0.0%	0	0.0%
	Total	6	3	1	0	7	3	4	57.1%	3	42.9%	3	42.9%

1.d.	If there are systems which have not yet been categorized, or, if a risk impact level was determined through another method, please explain: WBRS has not been categorized per FIPS 199, but a risk category was done during its January 2003 certification and accreditation. WBRS is scheduled to be incorporated into eSPAN by the end of the calendar year. The Salary Management System and HSPD-12 compliant Badge System have both recently be placed online after an initial assessment. A full assessment of both of these systems and WBRS in compliance with NIST guidelines is in processes. eSPAN's C&A has not yet been accepted by the approving authorities.
2.d.	If the number of systems with full certification and accreditation is higher than the number of systems with a tested contingency plan, please explain:

Question 3

Agencies must implement the recommended security controls in NIST Special Publication 800-53.

3.a.	Do you have a plan in place to fully implement the security controls recommended in NIST Special Publication 800-53? Yes or No.	**Yes**
3.b.	Have you begun to implement the security controls recommended in NIST Special Publication 800-53? Yes or No	**Yes**

Question 4

Incident Detection Capabilities.

4.a.	What tools, techniques, technologies, etc., does the agency use for incident detection? Response: Tools: McAfee Enterprise Suite, Web Root SpySweeper, Cisco Security Agent, Web Inspector & What's Up Gold Techniques: physical separation (Badging System); automatic notification, auto protect features	
4.b.	How many systems (or networks of systems) are protected using the tools, techniques and technologies described above?	Response: # 5 (WBRS is maintained by a contractor, badge system is not on a network)

Section B: Chief Information Officer. Question 5.

Agency Name: Corporation for National and Community Service

Question 5

Information gathered in this question will be forwarded to the Department of Homeland Security for validation.

For each category of incident listed: identify the total number of successful incidents in FY 05, the number of incidents reported to US-CERT, and the number reported to law enforcement. If your agency considers another category of incident type to be high priority, include this information in category e., "Other". If appropriate or necessary, include comments in the area provided below.

	5. Number of Incidents, by category:		
	Reported internally	Reported to US CERT	Reported to law enforcement
Type of Incident:	Number of Incidents	Number of Incidents	Number of Incidents
a. Unauthorized Access	0	0	0
b. Denial of Service (DoS)	0	0	0
c. Malicious Code	0	0	0
d. Improper Usage	0	0	0
e. Other (Virus)	30	0	0
Totals:	30	0	0

Comments:

Virus events were isolated to individual workstations and no outbreaks have occurred.

Section B: Questions 6 and 7 Question 6						
6. Has the agency ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities? Yes or No.						
a. Total number of employees in FY05	b. Number of employees that received IT security awareness training in FY 05, as described in NIST Special Publication 800-50, "Building an Information Technology Security Awareness and Training Program" (October 2003)		c. Total number of employees with significant IT security responsibilities	d. Number of employees with significant security responsibilities that received specialized training, as described in NIST Special Publication 800-16, "Information Technology Security Training Requirements: A Role- and Performance-Based Model" (April 1998)		Total costs for providing IT security training in FY05 (in $'s)
	Number	Percentage		Number	Percentage	
630	626	99%	5	3	60%	Spec Trng - $10,500; Awareness - $6,300
6.e. Briefly describe the training provided in b. and d:						
Comments: Yearly on line security awareness module provided to all employees and contractors with access to IT resources. Security Awareness costs determined per employee time to take the course (30 minutes average). Cisco firewall and other security related classes provided to OIT staff as part of the service agreement with Cisco. NIST two day training and conference held in July 2005 by entire security staff. Specialized security training costs are per staff that completed the courses and NIST two day training and conference in July 2005 attended by security staff.						
Question 7						
Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training? **Yes** or No.						Yes

Section B: Chief Information Officer. Question 8, 9, and 10. Agency Name: Corporation for National and Community Service		
Question 8		
8.a.	Is there an agency wide security configuration policy? Yes or No.	Yes
Comments: Since CNCS is a small agency all severs and workstation configuration are preformed within the Office of Infomration Technlogy and follow a standard configuration. All servers are configured based upon a set of standard configuration documentation. By using Norton Ghost, OIT ensures that all workstations are configured identically.		
8.b.	Configuration guides are available for the products listed below. Identify which software is addressed in the agency wide security configuration policy. Indicate whether or not any agency systems run the software. In addition, approximate the extent of implementation of the security configuration policy on the systems running the software.	

Product	**Addressed in agencywide policy?** **Yes, No, or N/A.**	**Do any agency systems run this software?** **Yes or No.**	**Approximate the extent of implementation of the security configuration policy on the systems running the software.** **Response choices include:** **- Rarely, or, on approximately 0-50% of the systems running this software** **- Sometimes, or on approximately 51-70% of the systems running this software** **- Frequently, or on approximately 71-80% of the systems running this software** **- Mostly, or on approximately 81-95% of the systems running this software** **- Almost Always, or on approximately 96-100% of the systems running this software**
Windows XP Professional	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Windows NT	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Windows 2000 Professional	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Windows 2000 Server	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Windows 2003 Server	N/A	No	
Solaris	N/A	No	

HP-UX	N/A	No	
Linux	N/A	No	
Cisco Router IOS	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Oracle	Yes	Yes	- Frequently, or on approximately 71-80% of the systems running this software
Other. Specify:			
Comments:			

Question 9

Indicate whether or not the following policies and procedures are in place at your agency. If appropriate or necessary, include comments in the area provided below.

9.a.	The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.	Yes
9.b.	The agency follows documented policies and procedures for external reporting to law enforcement authorities. Yes or No.	Yes
9.c.	The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov Yes or No.	Yes
Comments:		

Question 10

10.a.	Has the agency documented in its security policies special procedures for using emerging technologies (including but not limited to wireless and IPv6) and countering emerging threats (including but not limited to spyware, malware, etc.)? Yes or No.	No
10.b.	If the answer to 10 a. is "Yes," briefly describe the documented procedures. These special procedures could include more frequent control tests & evaluations, specific configuration requirements, additional monitoring, or specialized training.	
Response:		
Comments:		

Fiscal Year 2005 FISMA and Privacy Management Report

Office of Inspector General Narrative

During its review, the Office of Inspector (OIG) noted longstanding deficiencies with the Corporation's information security policies and procedures. In its response to our findings, Corporation management stated that it is fully aware of the importance of correcting these deficiencies and has made information security improvement a top priority. Specifically, it has embarked on a comprehensive plan of corrective action, which is due to be completed by March 1, 2006.

The OIG recognizes the level of commitment the Corporation has made to address our FISMA findings. The OIG will continue to closely monitor progress on this corrective plan and, if requested, will offer assistance to the Corporation.

Reporting Tab Note

CIO Tab B, Question 3.a., "Do you have a plan in place to fully implement the security controls recommended in NIST Special Publication 800-53?"

In his September 29, 2005 response to the FISMA narrative report, the Agency Chief Executive Officer transmitted a corrective action plan. That plan includes fully implementing the security controls recommended in NIST Special Publication 800-53. The OIG has not had the opportunity to review the Agency's detailed plan.

Section C: Inspector General. Questions 1, 2, 3, 4, and 5.

Agency Name: Corporation for National and Community Services, Inc. (Corporation)

Question 1 and 2

1. As required in FISMA, the IG shall evaluate a representative subset of systems, including information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. By FIPS 199 risk impact level (high, moderate, low, or not categorized) and by bureau, identify the number of systems reviewed in this evaluation for each classification below (a., b., and c.).

To meet the requirement for conducting a NIST Special Publication 800-26 review, agencies can:
1) Continue to use NIST Special Publication 800-26, or,
2) Conduct a self-assessment against the controls found in NIST Special Publication 800-53

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, therefore, self reporting by contractors does not meet the requirements of law. Self reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.

2. For each part of this question, identify actual performance in FY 05 by risk impact level and bureau, in the format provided below. From the representative subset of systems evaluated, identify the number of systems which have completed the following: have a current certification and accreditation , a contingency plan tested within the past year, and security controls tested within the past year.

		Question 1						Question 2					
		a. FY 05 Agency Systems		b. FY 05 Contractor Systems		c. FY 05 Total Number of Systems		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and evaluated in the last year		c. Number of systems for which contingency plans have been tested in accordance with policy and guidance	
Bureau Name	**FIPS 199 Risk Impact Level**	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
Bureau	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate	3	2	0	1	3	3	2	66.7%	0	0.0%	0	0.0%
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized	3	1	1	0	4	1	0	0.0%		0.0%		0.0%
	Sub-total	**6**	**3**	**1**	**1**	**7**	**4**	**2**	**50.0%**	**0**	**0.0%**	**0**	**0.0%**
Bureau	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Bureau	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Bureau	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Bureau	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Bureau	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Bureau	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Bureau	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Agency Totals	**High**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	#DIV/0!	**0**	#DIV/0!	**0**	#DIV/0!
	Moderate	**3**	**2**	**0**	**1**	**3**	**3**	**2**	66.7%	**0**	0.0%	**0**	0.0%
	Low	**0**	**0**	**0**	**0**	**0**	**0**	**0**	#DIV/0!	**0**	#DIV/0!	**0**	#DIV/0!
	Not Categorized	**3**	**1**	**1**	**0**	**4**	**1**	**0**	0.0%	**0**	0.0%	**0**	0.0%
	Total	**6**	**3**	**1**	**1**	7	**4**	**2**	50.0%	**0**	0.0%	**0**	0.0%

Question 3		
In the format below, evaluate the agency's oversight of contractor systems, and agency system inventory.		
3.a.	The agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy. Self-reporting of NIST Special Publication 800-26 requirements by a contractor or other organization is not sufficient, however, self-reporting by another Federal agency may be sufficient. Response Categories: - Rarely, for example, approximately 0-50% of the time - Sometimes, for example, approximately 51-70% of the time - Frequently, for example, approximately 71-80% of the time - Mostly, for example, approximately 81-95% of the time - Almost Always, for example, approximately 96-100% of the time	- Rarely, for example, approximately 0-50% of the time"
3.b.	The agency has developed an inventory of major information systems (including major national security systems) operated by or under the control of such agency, including an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency. Response Categories: - Approximately 0-50% complete - Approximately 51-70% complete - Approximately 71-80% complete - Approximately 81-95% complete - Approximately 96-100% complete	- Approximately 81-95% complete
3.c.	The OIG **generally** agrees with the CIO on the number of agency owned systems.	Yes
3.d.	The OIG **generally** agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency.	Yes
3.e.	The agency inventory is maintained and updated at least annually.	Yes
3.f.	The agency has completed system e-authentication risk assessments.	No

Question 4		
Through this question, and in the format provided below, assess whether the agency has developed, implemented, and is managing an agency wide plan of action and milestone (POA&M) process. Evaluate the degree to which the following statements reflect the status in your agency by choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the area provided below. For items 4a.-4.f, the response categories are as follows: - Rarely, for example, approximately 0-50% of the time - Sometimes, for example, approximately 51-70% of the time - Frequently, for example, approximately 71-80% of the time - Mostly, for example, approximately 81-95% of the time - Almost Always, for example, approximately 96-100% of the time		
4.a.	The POA&M is an agency wide process, incorporating all known IT security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency.	- Frequently, for example, approximately 71-80% of the time
4.b.	When an IT security weakness is identified, program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s).	- Frequently, for example, approximately 71-80% of the time
4.c.	Program officials, including contractors, report to the CIO on a regular basis (at least quarterly) on their remediation progress.	- Rarely, for example, approximately 0-50% of the time"
4.d.	CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	- Sometimes, for example, approximately 51-70% of the time
4.e.	OIG findings are incorporated into the POA&M process.	- Mostly, for example, approximately 81-95% of the time
4.f.	POA&M process prioritizes IT security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources	- Rarely, for example, approximately 0-50% of the time"
Comments:		

Question 5		
OIG Assessment of the Certification and Accreditation Process. OMB is requesting IGs to provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. Agencies shall follow NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" (May, 2004) for certification and accreditation work initiated after May, 2004. This includes use of the FIPS 199 (February, 2004), "Standards for Security Categorization of Federal Information and Information Systems," to determine an impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans .		
	Assess the overall quality of the Department's certification and accreditation process. Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	- Poor
Comments: There are currently seven systems reported by the OIT staff. The OIG system is not under the purview of the agency OIT. Through this year's FISMA review the OIG found four systems that are not properly being developed or Certified or accredited prior to being put into production. Of the three systems reported by OIT as being FIPS 199 compliant, all three have been ready for appropriate DAA approval.		

Section B: Inspector General. Question 6, 7, 8, and 9. Agency Name: Corporation for National and Community Services, Inc (Corporation) Question 6		
6.a.	Is there an agency wide security configuration policy? Yes or No.	Yes
	Comments:	

6.b. Configuration guides are available for the products listed below. Identify which software is addressed in the agency wide security configuration policy. Indicate whether or not any agency systems run the software. In addition, approximate the extent of implementation of the security configuration policy on the systems running the software.

Product	**Addressed in agencywide policy?** **Yes, No, or N/A.**	**Do any agency systems run this software?** **Yes or No.**	**Approximate the extent of implementation of the security configuration policy on the systems running the software.** **Response choices include:** **- Rarely, or, on approximately 0-50% of the systems running this software** **- Sometimes, or on approximately 51-70% of the systems running this software** **- Frequently, or on approximately 71-80% of the systems running this software** **- Mostly, or on approximately 81-95% of the systems running this software** **- Almost Always, or on approximately 96-100% of the systems running this software**
Windows XP Professional	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Windows NT	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Windows 2000 Professional	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Windows 2000 Server	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Windows 2003 Server	N/A	No	
Solaris	N/A	No	
HP-UX	N/A	No	
Linux	N/A	No	
Cisco Router IOS	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Oracle	Yes	Yes	- Frequently, or on approximately 71-80% of the systems running this software
Other. Specify:			
Comments:			

Question 7		
Indicate whether or not the following policies and procedures are in place at your agency. If appropriate or necessary, include comments in the area provided below.		
7.a.	The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.	Yes
7.b.	The agency follows documented policies and procedures for external reporting to law enforcement authorities. Yes or No.	Yes
7.c.	The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov Yes or No.	Yes
Comments:		

Question 8		
8	Has the agency ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities? Response Choices include: - Rarely, or, approximately 0-50% of employees have sufficient training - Sometimes, or approximately 51-70% of employees have sufficient training - Frequently, or approximately 71-80% of employees have sufficient training - Mostly, or approximately 81-95% of employees have sufficient training - Almost Always, or approximately 96-100% of employees have sufficient training	- Mostly, or approximately 81-95% of employees have sufficient training

Question 9		
9	Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training? Yes or No.	Yes

Section D: Senior Agency Official for Privacy Agency Name: Corporation for National and Community Service	
I. Senior Agency Official for Privacy Responsibilities	
1. Can your agency demonstrate through documentation that the privacy official participates in all agency information privacy compliance activities (i.e., privacy policy as well as IT information policy)? Yes or No.	No
2. Can your agency demonstrate through documentation that the privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and comments under Circular A-19? Yes or No.	No
3. Can your agency demonstrate through documentation that the privacy official participates in assessing the impact of technology on the privacy of personal information? Yes or No.	No
Comments: The CNCS Privacy Offical has only recently been assigned these duties and an assessment on fully incorporating the privacy is being persued. PIAs have not been preformed for any systems; the Corporation will be doing PIAs.	
II. Procedures and Practices	
1. Does your agency have a training program to ensure that all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure? Yes or No.	No
2. Does your agency have a program for job-specific information privacy training (i.e., detailed training for individuals (including contractor employees) directly involved in the administration of personal information or information technology systems, or with significant information security responsibilities)? Yes or No.	No
3. Section 3, Appendix 1 of OMB Circular A-130 requires agencies conduct -- and be prepared to report to the Director, OMB on the results of -- reviews of activities mandated by the Privacy Act. In the chart below, please indicate by component (e.g., bureau, agency) which of the following reviews were conducted in the last fiscal year.	

Bureau	Section M Contracts	Records Practices	Routine Uses	Exemptions	Matching Programs	Training	Violations	Systems of Records	
CNCS									

4.	Section 208 of the E-Government Act requires that agencies (a.) conduct Privacy Impact Assessments under appropriate circumstances, (b.) post web privacy policies on their websites, and (c.) ensure machine-readability of web privacy policies.		
	a.	Does you agency have a written process or policy for:	
		(i.) determining whether a PIA is needed? Yes/No	No
		(ii.) conducting a PIA? Yes/No	No
		(iii.) evaluating changes in business process or technology that the PIA indicates may be required? Yes/No	No
		(iv.) ensuring that systems owners and privacy and IT experts participate in conducting the PIA? Yes/No	No
		(v.) making PIAs available to the public in the required circumstances? Yes/No	No
		(vi.) making PIAs available in other than required circumstances? Yes/No	No
	b.	Does your agency have a written process for determining continued compliance with stated web privacy policies? Yes/No	No
	c.	Do your public-facing agency web sites have machine-readable privacy policies (i.e., are your web privacy policies P3P-enabled or automatically readable using some other tool)? Yes/No	Yes
		(i.) if not, provide date for compliance:	N/A

Section B: Senior Agency Official for Privacy.

Agency Name: Corporation for National and Community Service

II. Procedures and Practices, Continued.

5. By bureau, identify the number of information systems containing Federally-owned information in an identifiable form. For the applicable systems, on how many have you conducted a Privacy Impact Assessment and published a Systems of Records Notice?

	a.			b.						c.					
	FY 05 Systems that contain Federally-owned information in an identifiable form			FY 05 Privacy Impact Assessments: total number requiring a Privacy Impact Assessment in FY 05 (systems that are new or have been substantially altered)			FY 05 Privacy Impact Assessments: number that have a completed Privacy Impact Assessment within FY 05			FY 05 Systems of Records Notices: By bureau: number of systems from which Federally-owned information is retrieved by name or unique identifier			FY 05 Systems of Records Notices: number of systems for which one or more Systems of Records Notice/s have been published in the Federal register		
Bureau Name	Agency Systems	Contractor Systems	Total number of Systems	Agency Systems	Contractor Systems	Total number of Systems	Agency Systems	Contractor Systems	Total number of Systems	Agency Systems	Contractor Systems	Total number of Systems	Agency Systems	Contractor Systems	Total number of Systems
CNCS	6	1	7	5	0	5	0	0	0	4		4	4		4
			0			0			0			0			0
			0			0			0			0			0
			0			0			0			0			0
			0			0			0			0			0
			0			0			0			0			0
			0			0			0			0			0
			0			0			0			0			0
			0			0			0			0			0
			0			0			0			0			0
			0			0			0			0			0
			0			0			0			0			0
			0			0			0			0			0
			0			0			0			0			0
			0			0			0			0			0
Agency Totals			7			7			0			4			4

5.d. Contact Information for preparer of Question 5: Vanessa Brown, CNCS, 202-606-6671, vbrown@cns.gov
Systems Requiring PIAs does not include the OIG Network and WBRS because the system will be incorporated into eSPAN in December 2005.

Question 6		
OMB policy (Memorandum 03-22) prohibits agencies from using persistent tracking technology on web sites except in compelling circumstances as determined by the head of the agency (or designee reporting directly to the agency head).		
6.a.	Does your agency use persistent tracking technology on any web site? Yes/No	No
6.b.	Does your agency annually review the use of persistent tracking? Yes/No	Yes
6.c.	Can your agency demonstrate through documentation the continued justification for and approval to use the persistent technology? Yes/No	No
6.d.	Can your agency provide the notice language used or cite to the web privacy policy informing visitors about the tracking? Yes or No.	Yes
III. Internal Oversight		
1.	Does your agency have current documentation demonstrating review of compliance with information privacy laws, regulations and policies? Yes or No.	No
	(i.) If so, provide the date the documentation was created:	MM/DD/YYYY
2.	Can your agency provide documentation demonstrating corrective action planned, in progress or completed to remedy identified compliance deficiencies? Yes or No.	Yes
	(i.) If so, provide the date the documentation was created:	9/29/2005
3.	Does your agency use technologies that allow for continuous auditing of compliance with stated privacy policies and practices? Yes or No.	No
	(i.) If so, provide the date the documentation was created:	MM/DD/YYYY
4.	Does your agency coordinate with the agency Office of Inspector General on privacy program oversight by providing to OIG the following materials:	
	(a.) compilation of the agency's privacy and data protection policies and procedures? Yes/No	No
	(b.) summary of the agency's use of information in identifiable form? Yes/No	No
	(c.) verification of intent to comply with agency policies and procedures? Yes/No	No
5.	Does your agency submit an annual report to Congress (OMB) detailing your privacy activities, including activities under the Privacy Act and any violations that have occurred? Yes or No.	No
	(i.) If so, when was this report submitted to OMB for clearance?	MM/DD/YYYY

Section D - Senior Agency Official for Privacy Agency Name: Corporation for National and Community Service IV. Contact Information			
	Name	Phone Number	E-mail Address
Agency Head	David Eisner	202-606-6737	deisner@cns.gov
Chief Information Officer	Peter Hill	202-606-6609	phill@cns.gov
Agency Inspector General	Carol Bates (acting)	202-606-9356	c.bates@cnsoig.gov
Chief Information Security Officer	Matthew Baum	202-606-6611	mbaum@cns.gov
Senior Agency Official for Privacy	Peter Hill	202-606-6609	phill@cns.gov
Chief Privacy Officer	Peter Hill	202-606-6609	phill@cns.gov
Privacy Advocate			
Privacy Act Officer	Vanessa Brown	202-606-6671	vbrown@cns.gov
Reviewing Official for PIA's	Peter Hill	202-606-6609	phill@cns.gov

AGENCY RESPONSE TO FY 2005 INDEPENDENT EVALUATION REPORT

Corporation for
NATIONAL & COMMUNITY SERVICE

September 29, 2005

Ms. Carol Bates
Acting Inspector General
Corporation for National and
Community Service
Suite 830
Washington, D.C. 20525

Dear Ms. Bates:

Thank you for the opportunity to comment on the Federal Information System Management Act (FISMA) review for 2005. The Corporation takes its responsibility for ensuring that its information systems and infrastructure are secure and meet FISMA requirements very seriously and is committed to resolving the identified issues and improving our FISMA process.

The report identified three issues that the OIG deems to be significant deficiencies:

1. the Corporation has not complied with Memorandum 03-18, Implementation Guidance for the E-Government Act of 2002 (Public Law 107-347,44 United States Code (U.S.C.) Chapter 36), by not performing a Privacy Impact Assessment (PIA) and reporting the results to OMB.

2. the Corporation's security self-assessments not following the guidance in NIST SP 800-26, Self-Assessment Guide for Information Technology Systems because: (1) the documentation to support the reported levels (level 1-5) is not presently available; and (2) E-SPAN security self-assessment is not finalized and approved; though, the certification and accreditation (C & A) package has been ready since December 2004.

3. the Corporation's certification and accreditation efforts are not compliant with the NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems.

We don't disagree with these findings and believe they can best be addressed together as part of a comprehensive plan as outlined below. In addition, we have contracted with a FISMA consultant to assist the Corporation in completing its plan by March 1, 2006. Specifically, we will review our systems using the following process.

System Review Process Summary

1. Inventory all Corporation computer systems
2. Determine if the asset is a significant system. Define all systems into the following
   a. Major Application (MA)
   b. General Support System (GSS)
   c. Minor Applications (systems that are neither a MA nor a GSS)

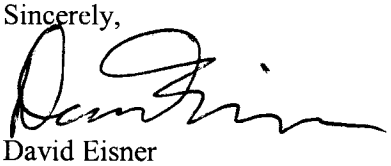
3. Categorize all required Systems based on the following:
    a. Identify the level of associated risk by evaluating –
        i. Functionality of the system
        ii. The types of data the system processes and holds
    b. Complete Privacy Impact Assessments (PIAs)
    c. Determine whether the system requires an E-Authentication Assessment
        i. Complete the E-Authentication Assessment when required
4. For All MA's or GSS will:
    a. Develop a controls baseline for the system
        i. Perform a Risk Assessment for the systems
    b. Develop a Security Plan for the systems.
    c. Perform an appropriate Security Test & Evaluation (ST&E)
    d. Complete an annual Self-Assessment
    e. Complete the C & A's
        i. Include the necessary documentation to ensure that the C & As are in compliance with OMB and NIST
        ii. Document the Rules of Behavior (ROB).
        iii. Document the Configuration Management baselines

We will complete the inventory and categorization by December 1, 2005.
We will complete this entire process by March 1, 2006.

The report also identified other issues that the Corporation has addressed in a separate response.

I would also like to express my appreciation for the efforts that your staff and the staff of Carson & Company made on the fiscal 2005 FISMA audit. Without this collaborative effort, we would not have been able to achieve the expedited deadline for completing the audit.

Sincerely,



David Eisner
Chief Executive Officer

General Response

In response to the problems related to the FISMA audit of last year, the Corporation invested more time this year with our FISMA contractor to improve the quality of the Certification and Accreditation's (C & A's). The Corporation instituted a policy of performing Certification and Accreditation's (C & A's) annually on all systems. This approach was adopted to ensure that the Corporation would be in compliance. After four iterations the resulting C & A's were significantly better than last year but not fully in compliance with NIST guidelines. To help ensure compliance on this as well as other items listed below, we have hired a new Contractor in order to help ensure that our C & As are fully compliant with NIST guidelines.

The Corporation is reviewing its OIT policy process in order to determine the optimal process to be used as we move forward. In addition, we will be reviewing our policies and procedures for FISMA compliance and add, or change them, where appropriate.

We will update or create our Corporate policies following the process outlined below.

1. Create a draft policy and implementation plan
2. Review the policy and Implementation plan with the Office of the CEO
3. Work with the Office of the CEO to determine who needs to sign off on the policy
4. Draft the final policy for sign-off
5. Submit the policy to the Office of the CEO for final reviewer determination
6. Initiate formal review process
7. Update the policy as appropriate
8. Implement the policy
9. Monitor for compliance

The following comments address each separate area identified in the 2005 FISMA report.

Risk Assessments

The revised SDLC policy, currently under review, incorporates more formal risk management practices that will address risk management processes and documentation requirements prior to the Corporation implementing new systems, system components, or services. The SDLC will be revised for sign off by December 1, 2005.

Risk assessments will be performed on all newly acquired or developed systems as indicated by NIST guidelines. We will update the RA process as part of an updated C & A process that will be identified during our review of all of our systems based upon FISMA and NIST guidelines in the process described below. We will be working with a FISMA contractor to complete this process on the dates referenced below.

System Review Process Summary

1. Inventory all Corporation computer systems
2. Determine if the asset is a significant system. Define all systems into the following
    a. Major Application (MA)
    b. General Support System (GSS)
    c. Minor Applications (systems that are neither a MA nor a GSS)
3. Categorize all required Systems based on the following:
    a. Identify the level of associated risk by evaluating –
        i. Functionality of the system
        ii. The types of data the system processes and holds
    b. Complete Privacy Impact Assessments (PIAs)
    c. Determine whether the system requires an E-Authentication Assessment
        i. Complete the E-Authentication Assessment when required
4. For All MA's or GSS will:
    a. Develop a controls baseline for the system
        i. Perform a Risk Assessment for the systems
    b. Develop a Security Plan for the systems.
    c. Perform an appropriate Security Test & Evaluation (ST&E)
    d. Complete an annual Self-Assessment
    e. Complete the C & A's
        i. Include the necessary documentation to ensure that the C & As are in compliance with OMB and NIST
        ii. Document the Rules of Behavior (ROB).
        iii. Document the Configuration Management baselines

We will complete the inventory and categorization by December 1, 2005.
We will complete this process by March 1, 2006.

We will revise our Risk Assessment to be compliant with NIST and tailored to fit our environment as identified during the system review process outlined above. We will add a list of participants to Section II, Risk Assessment Approach, for each RA.

The Corporation will review our risk management oversight and identify the appropriate improvements by March 1, 2006.

Security Policies and Procedures

The Corporation will review its online library to ensure that it is easily accessible by the appropriate people, up to date, easy to understand and in compliance with relevant Corporation, OMB, NIST and Federal mandates and guidelines by March 1, 2006. We will monitor the online library to ensure it is kept current.

We will monitor to ensure continued Corporation compliance with HSPD-12.

The Corporation will update our Information Security Policy #501 to support the current requirements of the Corporation's Network SSP and changes in NIST guidance.

The Corporation will update and formally approve Policy # 378 Structured Systems Development Life-Cycle Methodology by the second quarter FY 2006 including:

1. Identification of security personnel and notify them in writing of their assignment
2. Define IT security roles and responsibilities
3. Define procedures for disposal of media in the SDLC disposal phase and when no longer needed for data storage
4. Proper identification of security controls in accordance with NIST standards and guidance

The ISSO will update the Rules of Behavior to adequately address the requirements of the Major Applications and the General Support System. We will provide Corporation personnel with the Rules of Behavior for the GSS and the MAs they use. The Rules of Behavior will include information on the consequences of non-compliance.

The Corporation will review and revise its policy of performing C & A's every 12 months to meet the FISMA guidelines. We will include the appropriate criteria to determine when future C & As will be performed. We will consult with the IG to ensure that the Corporations definition and process for determining a significant change is compliant with NIST guidelines by March 1, 2006.

The following is a summary of the system review process:

System Review Process Summary

1. Inventory all Corporation computer systems
2. Determine if the asset is a significant system. Define all systems into the following
    a. Major Application (MA)
    b. General Support System (GSS)
    c. Minor Applications (systems that are neither a MA nor a GSS)
3. Categorize all required Systems based on the following:
    a. Identify the level of associated risk by evaluating –
        i. Functionality of the system
        ii. The types of data the system processes and holds
    b. Complete Privacy Impact Assessments (PIAs)
    c. Determine whether the system requires an E-Authentication Assessment
        i. Complete the E-Authentication Assessment when required
4. For All MA's or GSS will:
    a. Develop a controls baseline for the system
        i. Perform a Risk Assessment for the systems
    b. Develop a Security Plan for the systems.
    c. Perform an appropriate Security Test & Evaluation (ST&E)
    d. Complete an annual Self-Assessment
    e. Complete the C & A's
        i. Include the necessary documentation to ensure that the C & As are in compliance with OMB and NIST
        ii. Document the Rules of Behavior (ROB).
        iii. Document the Configuration Management baselines

We will complete the inventory and categorization by December 1, 2005.
We will complete this process by March 1, 2006.

System Security Plans

The Corporation will review all System Security Plans and update, as appropriate by March 1, 2006 in accordance with NIST SP 800-18.

The Corporation will update the Network SSP to indicate there are additional system-level ROBs to be adhered to in accordance with OMB (NIST Guidance).

The Corporation will update the Momentum SSP to include:

1. The identification and remediation of the planned controls;
2. The proper identification of the Disaster Recovery site;
3. Testing and the retention of test documentation;
4. Training requirements for personnel having disaster recovery responsibilities; and
5. Implement the recommendations.

The Corporation will review and determine the SSP summaries that should be included in its IT Strategic Plan.

Security Awareness and Training

The Corporation had planned to roll out a new security-training module on September 16, 2005, that incorporates text information regarding key areas of security awareness and asks questions directly linked to each topic area. Hot links and references to CNCS policies that are in force will be provided for the staff to view and read. The question must be answered correctly before the user can proceed to the next question. We have decided to review that module to ensure it addresses all of the needs and will release it on December 1, 2005.

The Corporation will review its security awareness and training prior to its release for:

1. The content of the security training program
2. Possible usurpation by employees
3. Tracking employee's progress throughout the training
4. Verifying that the user is aware of security treats and consequences.

In addition, to address current information security threats, we will begin sending out periodic emails to our user community with information about various security issues. We will also explore other ways to improve employee security awareness.

Annual Testing and Evaluation (SD)

The Corporation will be reviewing and modifying our policy on C & A's and self-assessments to schedule C & A's every three years or when there is a significant change to the system. We will revise our C & A policy to require a self-assessment as an attachment. During the years when a C & A is not required, we will conduct a self-assessment in accordance with NIST SP-26 or NIST SP 800-53.

As part of our new C & A policy we will define those conditions that determine a significant change. We will use these defined conditions as part of our change control process an impact assessment to determine whether a C & A is required.

The Corporation will continue to exploit established internal and external scanning procedures as a means of identifying network vulnerabilities and taking corrective action to mitigate risk.

We will ensure that any outstanding vulnerability identified in previous independent reviews are tracked properly as part of the Plan of Action and Milestones (POA&M's) and corrected as soon as possible.

Corrective Action Process (Plan of Action and Milestones)

The Corporation will review and change as needed our POA&M tracking and reporting process to comply with OMB guidelines and to ensure that all appropriate items make our POA&M list and are not removed until one year after items have been closed.

As part of our 2005 FISMA activities, we are propagating an IT security database focused on those items needed by our ISSO to help monitor the status of our IT program. When fully propagated, the database will contain a list of all Corporation systems, the categorization of each of those systems (Major Application, General Support System, Minor Application), what security documentation is required (e.g., PIA, C & A, self-assessment) and its status, and when each system is scheduled for a C & A review. In addition, the database will contain a consolidated listing of all IT security findings, their source, affected system or program, scheduled resolution date, and actual resolution date. This database will facilitate automated ISSO program oversight and will ensure that identified problem areas are resolved as scheduled. The database is scheduled to be operational by the December 30, 2005.

Continuity of Operations and Disaster Recovery

We will take appropriate steps to comply with NIST, OMB, or other Federal guidelines concerning contingency of operations and disaster recovery. These include:

- The Corporation will formally approve and test the COOP including training employees by May 1, 2006. We will document and retain the results.

- We will develop Contingency Plans for the facility, Major Applications, and General Support System, in accordance with NIST SP 800-34 and OMB guidance.

- We will update the Corporation's System Security Plan, Disaster Recovery Plan, and Momentum documentation on an annual basis, in compliance with NIST 800-34.

Configuration Management

The Corporation will review and update as required our draft Configuration Management Plan. We will ensure that all of our current configuration management processes are included in the plan. We will than formally accept the plan and use it as our operating guide for all of our Configuration processes by April 1, 2006.

Certification and Accreditation (C & A) (SD)

In addition to updating the C & A's policy, the Corporation will perform a C & A's on all MAs or GSS that have not had a C & A completed in the last three years. We will also review the categorization of all systems to ensure appropriate classification as a MA, GSS, or Minor system.

System Review Process Summary

1. Inventory all Corporation computer systems
2. Determine if the asset is a significant system. Define all systems into the following
    a. Major Application (MA)
    b. General Support System (GSS)
    c. Minor Applications (systems that are neither a MA nor a GSS)
3. Categorize all required Systems based on the following:
    a. Identify the level of associated risk by evaluating –
        i. Functionality of the system
        ii. The types of data the system processes and holds
    b. Complete Privacy Impact Assessments (PIAs)
    c. Determine whether the system requires an E-Authentication Assessment
        i. Complete the E-Authentication Assessment when required
4. For All MA's or GSS will:
    a. Develop a controls baseline for the system
        i. Perform a Risk Assessment for the systems
    b. Develop a Security Plan for the systems.
    c. Perform an appropriate Security Test & Evaluation (ST&E)
    d. Complete an annual Self-Assessment
    e. Complete the C & A's
        i. Include the necessary documentation to ensure that the C & As are in compliance with OMB and NIST
        ii. Document the Rules of Behavior (ROB).

iii. Document the Configuration Management baselines

We will complete the inventory and categorization by December 1, 2005.
We will complete this process by March 1, 2006.

We will complete the process for this years C & A to grant the appropriate ATO for eSpan.

In addition, we will provide the appropriate line of secession for system notification within the C & A letters. We put in place a process to notify all stakeholders of any significant change to the Corporation's security posture due to a significant change or addition of hardware or software that requires new C & A efforts.

Privacy (SD)

As part of our C & A process, described in our general comments under system categorization, we will Complete Privacy Impact Assessments (PIAs) on all of the systems currently within the Corporation's operational boundaries and under development. We will complete a PIA on any new system before it goes live. As part of any new C & A we will revisit the existing PIA.

In addition, we will conduct and make available E-Authentication assessments for the Corporation's systems to determine compliance with OMB requirements.