Office of Inspector General
Corporation for National and
Community Service

INDEPENDENT EVALUATION OF CORPORATION FOR NATIONAL AND COMMUNITY SERVICE COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2004

OIG REPORT NUMBER 05-07

Corporation for
NATIONAL &
COMMUNITY
SERVICE

Prepared by:

Richard S. Carson & Associates
4720 Montgomery Lane, Suite 800
Bethesda, MD 20814-3444

This report was issued to Corporation management on October 6, 2004. Under the laws and regulation governing evaluation follow-up, the Corporation must make final management decisions on the report's findings and recommendations not later than April 6, 2005 and complete it corrective actions by October 6, 2005. Consequently, the report findings do not necessarily represent the final resolution of the issues presented.

BACKGROUND

This report provides the results of the independent evaluation of the Corporation's information security program conducted by Richard S. Carson & Associates, Inc. (Carson Associates) on behalf of the Office of Inspector General (OIG), Corporation for National and Community Service (Corporation).

The independent evaluation was undertaken to support the OIG's statutory responsibility to assess the Information Technology (IT) security posture of the Corporation, as mandated by the Federal Information Security Management Act of 2002 (FISMA).

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

RESULTS IN BRIEF

The Corporation has taken a number of steps to enhance its security program and address issues identified in the 2003 FISMA report. The Corporation has made the following enhancements:

- Provided staff access to a comprehensive library of current policies and procedures via the Corporation's Intranet.
- Initiated a proactive security awareness program.
- Conducted periodic network scans to identify vulnerabilities and take appropriate steps to mitigate risk.
- Installed an effective security incident reporting process that follows United States Computer Emergency Response Team (US-CERT) policies.
- Completed effective configuration management of Corporation systems and assets.

However, one area showed little progress toward remediation and/or did not adhere to Office of Management and Budget (OMB) Circular A-130 guidance. In this regard, the following conclusion and finding was considered a significant deficiency:

- The Corporation's major applications and general support system security have not undergone complete testing and evaluation in the past 12 months, resulting in noncompliance with FISMA in the area of annual testing and evaluation.

RECOMMENDATIONS

The independent evaluation resulted in 17 recommendations requiring corrective action. The consolidated list of these recommendations begins on page 11.

AGENCY COMMENTS

At the exit conference held on August 17, 2004, Corporation officials generally agreed with the findings. Upon review of the draft report, Corporation officials provided a formal response on October 5, 2004, which is included as Appendix C.

The response provided by Corporation officials disagrees with the significant deficiency rendered in the area of annual testing and evaluation. The points raised by Corporation officials were thoroughly considered during the independent assessment and are fully discussed in the conclusions and findings related to annual testing and evaluation. The independent assessment determined that a significant deficiency was warranted based on the systemic nature of the weakness and the attendant risk of noncompliance with a significant management control mandated by FISMA.

ABBREVIATIONS AND ACRONYMS

ASSET	Automated Security Self-Evaluation Tool
C&A	Certification and Accreditation
CFO	Chief Financial Officer
CIO	Chief Information Officer
CM	Configuration Management
COTS	Commercial Off-the-Shelf
DOI	Department of the Interior
e-Grants	Electronic-Grants
E-SPAN	Electronic-System for Program Agreements and National Service Participants
FISCAM	Federal Information System Controls Audit Manual
FedCIRC	Federal Computer Incident Response Center
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GAO	Government Accountability Office
GSS	General Support System
HSPD	Homeland Security Presidential Directive
IG	Inspector General
ISSO	Information Systems Security Officer
IT	Information Technology
LAN	Local Area Network
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
SAINT®	System Administrator's Integrated Network Tool
SDLC	Systems Development Life Cycle
SP	Special Publication
TBD	To Be Determined
US-CERT	United States Computer Emergency Readiness Team
WBRS	Web-Based Reporting System

TABLE OF CONTENTS

Appendices

Background

Richard S. Carson & Associates, Inc. (Carson Associates), 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. This report provides conclusions and findings, identifies problem areas, where applicable, and makes recommendations based on our independent evaluation. Conclusions, findings, and recommendations are based on an evaluation of compliance with the E-Government Act of 2002 (Public Law No. 107-347) and other Federal guidelines.

Title III of the E-Government Act of 2002, the Federal Information Security Management Act of 2002 (FISMA), was enacted to strengthen the security of Federal Government information and information systems. The FISMA outlines information security compliance criteria for agencies, including the requirement for annual review and independent assessment by agency inspectors general. Mandated annual assessments provide agencies with the information needed to determine security program effectiveness and to establish strategies and best practices for improving information security.

This independent evaluation addresses the Corporation's:

- information security program;
- progress towards correcting weaknesses identified in prior FISMA reports and attendant Plans of Action and Milestones (POA&Ms);
- review of agency self-assessments; and
- verification and testing of information security controls of agency information systems.

The results of the independent evaluation are presented in subsequent discussions of risk assessments, security policies and procedures, system security plans, security awareness and training, annual testing and evaluation, corrective actions, security incident reporting, continuity of operations, and configuration management.

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 and General Support System (GSS);
- Assess Corporation compliance with FISMA and related information security policies, procedures, standards and guidelines; and
- Assess Corporation progress in correcting weaknesses identified in the Fiscal Year (FY) 2003 POA&M.

This independent evaluation report is a stand-alone document, which establishes the basis for reporting the FY 2004 Information Technology (IT) security posture of the Corporation to the Office of Management and Budget (OMB).

The independent evaluation was conducted in accordance with generally accepted government auditing standards. All applicable standards were followed.

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 OMB, the National Institute of Standards and Technology (NIST), and applicable policies, procedures, standards, and guidelines (criteria) is cited when describing a specific conclusion and finding (condition). When appropriate, the root cause and effect of the conclusion and finding is discussed. Each conclusion and finding has corresponding recommendations. These recommendations are intended to assist the Corporation in determining the action needed to correct weaknesses and/or deficiencies.

Agency Risk Assessments

Conclusions and Findings

Risk assessments were conducted as part of the Certification and Accreditation (C&A) of the Corporation's GSS (Corporation Network) and its major applications: Momentum, Electronic-System for Program Agreements and National Service Participants (E-SPAN), and Electronic-Grants (e-Grants). OMB Circular A-130 requires that every information system undergo C&A at least every three years, or when a significant change takes place. The circular further requires that Federal agencies include a risk assessment in the C&A process. The NIST provides guidance on how to develop a risk assessment.[1] The Corporation's risk assessments of major applications and the Corporation Network follow NIST guidelines with one omission: the risk assessments do not identify the names of participants involved in developing the risk assessments. The soundness of the risk assessments rests on the authoritative knowledge of the participants. By not identifying the participants, the Corporation places the validity and credibility of the risk assessments in question.

Recommendations

Based on conclusions and findings associated with agency risk assessments, we recommend that the Corporation:

- Conduct C&As at least every three years, or when a significant change takes place, to ensure the Corporation's major applications and Corporation Network continue to have "authorization to operate."[2]
- Add the names and titles of participants to Section II, Risk Assessment Approach, NIST SP 800-30, for each risk assessment.

[1] NIST Special Publication (SP) 800-30, *A Risk Management Guide for Information Technology Systems* (2004).

[2] The phrase "authorization to operate" refers to the accreditation decision rendered by the authorizing official to approve full operation of an information system in accordance with NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems* (2004).

Security Policies and Procedures

Conclusions and Findings

The Corporation has a comprehensive library of current policies and procedures available to staff through its Intranet. Policies include guidelines for obtaining accounts to access the network, obtaining security awareness training, 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 to respond to a system failure. This library of policies and procedures gives employees a quick and easy reference for handling security matters.

The Corporation has complied with Development of Homeland Security Presidential Directive M-04-15 (HSPD)-7, *Critical Infrastructure Identification, Prioritization and Protection.* The HSPD–7 supersedes Presidential Decision Directive/National Security Council -63. The HSPD-7 requires Federal departments and agencies to prepare plans for protecting physical and cyber-critical infrastructure and key resources by July 31, 2004. On July 12, 2004, the Corporation responded to the directive by indicating that the Corporation falls into the category of a small agency. The Corporation cited its major business function as making grants to nonprofits and State and local government agencies. The Corporation further noted that the Department of Health and Human Services Payment Management System and Department of the Interior (DOI) National Business Center actively maintain the critical infrastructure used by the Corporation to operate Momentum. In addition to providing the critical infrastructure and key resources protection, the National Business Center also serves as the Corporation's alternate disaster recovery site. Compliance with the directive ensures that the Corporation's critical infrastructure and key resources are identified for OMB compilation of threat vulnerability information.

The current System Development Life Cycle (SDLC) does not include a methodology to dispose of hardware or software. The NIST outlines five distinct SDLC phases: initiation, acquisition/ development, implementation, operation/maintenance, and disposition.[3] The Corporation includes the first four phases in its SDLC, but does not address the fifth phase, disposition. Improper disposal of hardware or software may result in the exploitation of residual data of a personal and/or sensitive nature, leading to Privacy Act violations or other compromises of sensitive data.

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 Circular A-130 and NIST guidelines call for establishment of security measures throughout a system's life cycle.[4] In today's computing environment, many agency systems use products that can offer advanced capabilities without extensive customization by technical staff. However, while such capabilities are not developed by the agency, these products are integrated into the collective architecture and have a major impact on security configurations and practices. Therefore, COTS products should be addressed in the Corporation's SDLC documentation. The lack of common criteria for evaluating COTS software can lead to incompatible software within the Corporation's architecture and introduce security risks. It should be noted that a new draft SDLC that addresses this concern is pending formal approval.

Recommendations

Based on conclusions and findings associated with security policies and procedures, we recommend that the Corporation:

[3] NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle* (2004).

[4] *Id.*

- Incorporate a disposal phase into SDLC documentation in accordance with NIST SP 800-64.
- Complete the approval process for the new draft SDLC as soon as possible.

System Security Plans

Conclusions and Findings

Although the Corporation Network security plan presents current and planned controls for ensuring protection of the Corporation Network, the plan does not include a list of previously conducted security control reviews. The Corporation Network security plan generally conforms to OMB Circular A-130 and NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems.* The NIST standards direct agencies to "[d]escribe the type of review and findings conducted on the general support system or major application in the last three years" and to "[i]nclude information about the last independent audit or review of the system and who conducted the review."[5] The Corporation Network security plan does not address previously conducted control reviews. This omission can lead to duplication of effort and a waste of time and money.

Corporation Policy #501, *Safeguarding Sensitive Information and Documents*, is not universally understood or followed by agency personnel. Corporation Policy #501 establishes guidelines for safeguarding sensitive information and documents. While conducting site surveys, a number of infractions of the policy were noted. Infractions did not appear to be widespread or endemic, but various independent failures were discovered at different office locations. Those personnel who were in violation did not seem to fully appreciate or understand the ramifications of their actions. Such lapses could create a lax security climate, ultimately jeopardizing the agency's security posture.

A summary of major application security plans is not included in the Corporation's Information Technology (IT) Strategic Plan. This finding was also cited in the FY 2003 FISMA Report. OMB Circular A-130 requires that "[a] summary of the security plans shall be incorporated into the strategic Information Resource Management plan required by the Paperwork Reduction Act (44 U.S.C. Chapter 35)."[6] Noncompliance with the referenced requirement denies senior officials visibility on system security information for long-range budget and IT capital planning purposes.

Recommendations

Based on conclusions and findings associated with system security plans, we recommend that the Corporation:

- Update the system security plan to reflect previously conducted security control reviews.
- Emphasize Corporation Policy #501 as part of the Corporation's security awareness program.
- Include system security plan summaries in the IT Strategic Plan.

[5] NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*, 4.2 (1998).
[6] OMB Circular A-130, *Management of Federal Information Resources*, Appendix III, § A(3)(a)(2).

Security Awareness and Training

Conclusions and Findings

The Corporation maintains a proactive security awareness program, ensuring all employees and contractors with system access undergo annual security awareness training. The Computer Security Act of 1987 required agencies to provide security awareness training for all employees.[7] The FISMA updated this training requirement.[8] The Corporation's security awareness program fully conforms to the FISMA and OMB guidelines. Corporation policy requires new users to complete security awareness training prior to receiving authorization to access the network. Upon notification of successful completion, the Office of Information Technology (OIT) Help Desk and Information Systems Security Officer (ISSO) create new accounts and issue one-time temporary passwords.

The Corporation's new policy on passwords, dated June 1, 2004, requires new users to change their passwords after initial log in. The new policy has stringent password requirements and enforces new password complexity rules.

The ISSO maintains a database of all user security awareness training and proactively prompts users when annual training is due. Procedures are also in place for employee training prior to obtaining accounts and gaining access to major applications and sensitive information, as well as for accounts that can be inactivated and retired. Training material is conveniently available to users online and classroom instruction is also conducted. Additionally, online instructions are available to users on how to report security incidents and what their responsibilities are in those instances. The ISSO and OIT Help Desk provide users with information regarding current security concerns, such as United States Computer Emergency Readiness Team (US-CERT) virus alerts.

Recommendations

Based on conclusions and findings associated with security awareness and training, we recommend that the Corporation:

- Enhance security awareness training by informing users of current information threats and network vulnerabilities.

Annual Testing and Evaluation

Conclusions and Findings

The Corporation's major applications and general support system security have not undergone complete testing and evaluation in the past 12 months, resulting in noncompliance with FISMA in the area of annual testing and evaluation. This is considered a significant deficiency. The FISMA requires at least annual testing and evaluation of the effectiveness of information security policies, procedures, and practices to ensure that system environments remain secure.[9] The NIST guidelines provide the criteria for conducting annual self-assessments that meet the requirement for annual testing and evaluation.[10] However, the Corporation's stated practice is to perform annual C&As in lieu of self-assessments. The criteria that meets the FISMA requirement consists of:

[7] Pub. L. No. 100-235.

[8] 44 U.S.C. § 3534(a)(3)(D).

[9] *See* 44 U.S.C. § 3534 (b)(5).

[10] NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems* (2001).

- Determining agency security status within the five levels of security defined by NIST SP 800-26;
- Examining at least 17 control areas of those outlined in NIST SP 800-26 (e.g., identification and authentication, contingency planning, etc.);
- Providing control objectives and techniques that can be measured for each area; and
- Determining if additional security controls should be added to the self-assessment in addition to those identified in NIST SP 800-26.

No C&As were completed by the Corporation in the last 12 months. Momentum and the Corporation Network C&As were last completed on November 25, 2002. Certification and accreditations of E-SPAN and e-Grants were completed on January 6, and January 20, 2003, respectively. Additionally, no self-assessments were conducted since the C&As of November 2002 and January 2003. It is acknowledged that the Corporation used the NIST Automated Security Self-Evaluation Tool (ASSET) to assist in conducting annual reviews in September 2003.[11] However, the use of ASSET alone does not meet the criteria for an annual self-assessment. NIST guidelines state that:

> It is important to note that the questionnaire is not intended to be an all-inclusive list of control objectives and related techniques. Accordingly, it should be used in conjunction with the more detailed guidance listed in Appendix B. In addition, details associated with certain technical controls are not specifically provided due to their voluminous and dynamic nature. Agency managers should obtain information on such controls from other sources, such as vendors, and use that information to supplement this guide.[12]

Additionally, the September 2003 ASSET was supported by information from the November 2002 C&As. The Corporation could not provide documentation to show that more current information was used. The ASSET reports also had errors and noted some weaknesses that were not included in the POA&Ms. The NIST guidelines emphasize using the tool to correct weaknesses. No information was provided to show the Corporation used the ASSET results to improve information security. Other than ASSET reports, the Corporation did not have documentation to validate and verify annual system reviews.

Failure to conduct, document, and retain the results of annual testing and evaluation of management, operational, and technical controls permits new threats and vulnerabilities to go undetected for an extended period of time. Furthermore, the absence of annual testing and evaluation poses high risk to the Corporation's information security environment.

The Corporation has not documented its stated practice of performing annual C&As to meet the FISMA requirement for annual testing and evaluation of system security. This finding was also cited in the 2003 FISMA Report. The FISMA requires at least annual testing and evaluation of the effectiveness of information security policies, procedures, and practices to ensure that system environments remain secure.[13] The Corporation has opted to establish an annual C&A process in lieu of annual self-assessments. This was the stated practice during the FY 2003 Independent Audit, which recommended that the practice be documented, because undocumented procedures could result in failure

[11] The ASSET is an automated IT security questionnaire developed by the NIST to support self-assessments. The tool is available for downloading at http://csrc.nist.gov/asset/.
[12] NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems* (2001).
[13] *See* 44 U.S.C. § 3534 (b)(5).

to perform annual testing and evaluation. The practice has not yet been established in writing, and the potential adverse effect of failing to perform annual testing and evaluation remains a valid concern.

The Corporation scans its general support system network to identify vulnerabilities and takes appropriate steps to mitigate risk. Staff from the OIT conduct internal scanning using specialized scanning software. The staff perform detailed vulnerability scans of Corporation system architecture to identify issues such as update requirements, 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 to ensure the configuration is secure and meets current configuration management requirements for the network. The OIT methodology includes performing system changes and updates on a test platform and re-running applicable scans to validate changes prior to their deployment.

Outside consultants also perform internal and external scanning in conjunction with the FISMA independent evaluation. The FY 2004 internal and external vulnerability assessment was conducted from July 7 to July 22, 2004, using a variety of tools. Scanned data was analyzed and the results forwarded to the Corporation for appropriate follow-up action. Once delivered, all data and products were removed from the consultants' laptops.

Recommendations

Based on conclusions and findings associated with annual testing and evaluation, we recommend that the Corporation:

- Conduct annual self-assessments in accordance with NIST SP 800-26, or
- Document and enforce the stated practice of annual C&As to meet the FISMA requirement for testing and evaluation every 12 months.
- Document standard procedures for scanning activities.

Corrective Action Process

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 findings included in the FISMA Review for FY 2003. The POA&M now captures individual POA&M items, as well as summary-level information. The refined process tracks IT security weaknesses identified through the various audits, assessments, and testing events. The Deputy Chief Information Officer (CIO) has also implemented system-level tracking. The next focus should be to improve POA&M annotations. Details from the various audits, C&As, and independent evaluations are not being recorded in the POA&M, causing relevant information to be overlooked in the tracking process. Consequently, various agency process owners and stakeholders may have IT security weaknesses that do not receive adequate attention or proper resolution.

While the Corporation has established a single, agency-wide POA&M, as recommended in the FISMA Review for FY 2003, the POA&M has not been maintained in accordance with OMB guidance which requires a baseline POA&M. Submission guidelines from OMB require agencies to establish a baseline POA&M.[14] Once the initial POA&M is completed, no changes should be made to the

[14] OMB Memorandum, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*

data entered in columns 1, 4, 5, and 7. Verification and validation of the POA&M report to OMB revealed items in column 4 (scheduled completion date) and column 5 (key milestones with completion dates) that were adjusted from quarter to quarter. The effect is that follow-up progress on POA&M items cannot be adequately monitored. As a consequence of this conclusion and finding, the Corporation has established that the June 15, 2004, 3rd Quarter POA&M submission will serve as the baseline POA&M.

Recommendations

Based on conclusions and findings associated with the corrective action process, we recommend that the Corporation:

- Improve the current single, agency-wide POA&M process by tracking all reported weaknesses until closed.
- Maintain the June 15, 2004, 3rd Quarter POA&M in accordance with OMB submission guidelines requiring that data in columns 1, 4, 5, and 7 remains fixed, to serve as the baseline for subsequent quarterly updates.

Security Incident Reporting

Conclusions and Findings

The Corporation has developed and maintains an effective security incident reporting process that follows United States Computer Emergency Response Team (US-CERT) policies.[15] OMB Circular A-130 requires that all agencies develop an incident response capability for their major applications and general support systems.[16] The Corporation maintains a detailed policy available to all users through the Corporation Intranet. It provides guidance concerning security incident reporting procedures and responsibilities. The Deputy CIO and ISSO take an active role in this process, particularly for IT-related incident reporting. The Deputy CIO is knowledgeable regarding what types of incidents are considered reportable and the procedures used to invoke the reporting process. In the past year, no incidents at the Corporation Headquarters, its Service Centers, or State offices have required the report of a serious incident.

Incidents of threats to physical security are the responsibility of Administrative Services. Physical security notification procedures require incidents to be reported immediately. If the incident takes place within Headquarters, Administrative Services contacts the Federal Protective Service, which responds to the incident. The respective local police departments are contacted for response to incidents outside Headquarters.

Continuity of Operations

Conclusions and Findings

The continuity of operations plans for the major applications and general support system reviewed during this assessment have undergone testing as part of their C&As. The NIST guidelines call for contingency plans to contain detailed records of system configurations in order to enhance system

(2004).

[15] In March 2004, the Federal Computer Incident Response Center (FedCIRC) was reassigned to US-CERT.

[16] OMB Circular A-130, Management of Federal Information Resources, Appendix III § A(3)(a)(2)(d).

recovery capabilities.[17] The Corporation uses a combination of documents (primarily the contingency plan for a given system in conjunction with the Corporation's disaster recovery plan) to ensure mission critical operations are maintained and systems restored. The disaster recovery plan, dated August 2003, is well written and generally adheres to NIST guidelines.

However, several discrepancies in the disaster recovery plan were noted. In Section 1.3, Recovery Organization, disaster recovery team responsibilities were listed as "TBD at a later date." In Section 1.4, OIT Responsibilities Summary, Windows NT is the stated operating system, but the Corporation uses the Windows 2000 platform. In Section 2.2, Active Recovery Team, the Corporation's organizational chart remains "TBD." The disaster recovery plan should be revised to correct these deficiencies.

The Corporation Network Contingency Plan, dated August 2001, does not fully follow NIST guidelines. There are a number of discrepancies. To name several, the Contingency Plan fails to establish an authority line of succession. Additionally, notification procedures for recovery personnel to respond during business and non-business hours are not specified. While personnel are listed in the document, their roles and responsibilities are not clearly defined, or the personnel are either no longer employed by the Corporation or have been reassigned.

The Corporation has been proactive in following the recommendations contained in the Momentum Contingency Plan Report, dated November 25, 2002. The report provides an evaluation of the existing Contingency Plan for Momentum, which is maintained by the National Business Center, a DOI organization. Momentum's disaster recovery plan conforms to FISMA requirements by adequately describing the strategy for recovery. This strategy provides for the establishment of an alternate processing site, documents the decision-making process, and identifies critical functions, processes, resource needs, and roles and responsibilities for emergency response, backup operations, and recovery operations. All recommendations in the Momentum Contingency Plan Report had been completed by the time the report was published. No significant security concerns were reported. The National Business Center last tested the disaster recovery plan and the contingency plan in August 2003.

The e-Grants resources noted in the FISMA Review for FY 2003 have been acquired and installed at the alternate disaster recovery site. The Deputy CIO confirms the acquisition and installation of the equipment, but indicates this equipment has not been, and will not be, fully tested due to cost considerations and the need for the Corporation to declare a disaster to fully conduct the tests. A limited contingency plan test was conducted at Corporation Headquarters in September 2003, but the alternate disaster recovery site was not tested. Test results were not retained. The testing scenario was interrupted by a live recovery operation. The Deputy CIO described the incident as follows:

> A failure occurred when our tape drive died during a data restore. This forced us to acquire a new tape drive from a vendor overnight to complete our testing as scheduled. We were successful in completing the testing as scheduled. This actually demonstrated that we have appropriate restore procedures in place as well as procurement vehicles. I like to think of this as an added bonus.

This live failure afforded the Corporation an opportunity to assess the viability of the contract in place for obtaining replacement parts in an emergency. The hardware components were delivered and installed within 24 hours, as required by the contract, demonstrating an acceptable recovery response. Should a similar failure occur at the alternate disaster recovery site, it is anticipated that the Corporation would receive the same responsive contract support.

[17] NIST SP 800-34, Contingency Planning Guide for Information Technology Systems (2002).

Recommendations

Based on conclusions and findings associated with continuity of operations, we recommend that the Corporation:

- Update the Corporation's disaster recovery plan and contingency plan, as necessary, to meet NIST SP 800-34 guidelines.
- Retain continuity of operations plan test results for examination by future audits, reviews, and independent evaluations.
- Formally document that the alternate disaster recovery site for e-Grants was not being tested, and issue a letter of acceptance of risk for senior management approval.

Configuration Management

Conclusions and Findings

Configuration Management (CM) of Corporation systems and assets is performed in an effective manner, but the process has not been formalized. The NIST guidelines state that managing and monitoring are key components of systems configuration.[18] In this regard, the Corporation has implemented many configuration management 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 Section 305 of the FISMA.[19] 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 with CIO and Deputy CIO involvement in security issues. The configuration control board recommendations that have budget implications must be approved by the Chief Financial Officer (CFO). The OIT also utilizes computer-aided software engineering tools from Oracle to design, develop, and maintain security settings and database roles or permissions within application databases. To further enhance the Corporation's configuration management program, a formal written configuration management plan should be developed. The configuration management plan would combine many activities into a single, integrated process, providing greater managing and monitoring benefits.

Recommendations

Based on conclusions and findings associated with configuration management, we recommend that the Corporation:

- Develop a configuration management plan and obtain senior management approval.

[18] NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle, Revision 1* (2004).
[19] This FISMA requirement is codified at 44 U.S.C. § 3505(c).

Consolidated List of Recommendations

Agency Risk Assessments:

- Conduct C&As at least every three years, or when a significant change takes place, to ensure the Corporation's major applications and Corporation Network continue to have "authorization to operate."

- Add the names and titles of participants to Section II, Risk Assessment Approach, NIST SP 800-30, for each risk assessment.

Security Policies and Procedures:

- Incorporate a disposal phase into the SDLC documentation in accordance with NIST SP 800-64.

- Complete the approval process for the new draft SDLC as soon as possible.

System Security Plans:

- Update the system security plan to reflect previously conducted security control reviews.

- Emphasize Corporation Policy #501 as part of the Corporation's security awareness program.

- Include system security plan summaries in the IT Strategic Plan.

Security Awareness and Training:

- Enhance security awareness training by informing users of current information threats and network vulnerabilities.

Annual Testing and Evaluation:

- Conduct annual self-assessments in accordance with NIST SP 800-26, or

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

- Document standard procedures for scanning activities.

Corrective Action Process:

- Improve the current single, agency-wide POA&M process by tracking all reported weaknesses until closed.

- Maintain the June 15, 2004, 3rd Quarter POA&M in accordance with OMB submission guidelines requiring that data in columns 1, 4, 5, and 7 remains fixed, to serve as the baseline for subsequent quarterly updates.

Continuity of Operations:

- Update the Corporation's disaster recovery plan and contingency plan, as necessary, to meet NIST SP 800-34 guidelines.

- Retain continuity of operations plan test results for examination by future audits, reviews, and independent evaluations.

- Formally document that the alternate disaster recovery site for e-Grants was not being tested, and issue a letter of acceptance of risk for senior management approval.

Configuration Management:

- Develop a configuration management plan and obtain senior management approval.

Response to Agency Comments

At the exit conference held on August 17, 2004, Corporation officials generally agreed with the findings. Upon review of the draft report, Corporation officials provided a formal response on October 5, 2004, which is included as Appendix C.

The response provided by Corporation officials disagrees with the significant deficiency rendered in the area of annual testing and evaluation. The points raised by Corporation officials were thoroughly considered during the independent assessment and are fully discussed in the conclusions and findings related to annual testing and evaluation on page 6.

In summary, the independent assessment found that the Corporation failed to conduct C&As or complete self-assessments in the last 12 months. Although ASSET reports were prepared in September 2003, the use of this tool exclusively does not constitute an annual self-assessment. The Corporation provided no information to demonstrate that management acted upon ASSET reports to improve information security. Additionally, the ASSET reports contained outdated information from the C&As conducted in 2002. The Corporation could not provide documentation to show that more current information was used. The ASSET reports also contained errors and noted certain weaknesses that were not included in the POA&Ms. Other than the ASSET reports that were based on outdated information, the Corporation had no other documentation to verify annual system reviews.

Therefore, the independent assessment determined that a significant deficiency was warranted based on the systemic nature of the weakness and the attendant risk of noncompliance with a significant management control mandated by FISMA. At this time, the Corporation's annual testing and evaluation policy is not codified, and the process by which the Corporation intends to comply with the FISMA requirement for annual testing and evaluation remains unclear. The disputed significant deficiency can be addressed through the POA&M process.

OBJECTIVE, SCOPE AND METHODOLOGY

The overall objective of this independent evaluation was to assist the OIG in meeting its FISMA obligation to conduct an independent assessment of the Corporation's information security in accordance with OMB guidelines.[20] The evaluation team conducted a high-level, qualitative review of the Corporation's information security program. It specifically evaluated the agency's degree of compliance with applicable criteria for a security program, and the effectiveness of automated and manual security controls for three of the Corporation's mission-essential systems. Systems examined were:

- Momentum;
- E-SPAN (e-Grants as a module of E-SPAN); and
- The Corporation Network.

The following systems and sites were not included in the scope of this independent evaluation:

- The Web-Based Reporting System (WBRS);
- The OIG Local Area Network (LAN); and
- Contractor-operated facilities.

The scope of work was organized into three tasks:

- Background review;
- Evaluation fieldwork; and
- Evaluation reporting.

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

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

- The Deputy CIO (representing the Agency Head, CIO, Program Officials, and System Administrator);
- The ISSO;
- Selected OIG staff members; and
- Selected system users.

[20] OMB Memorandum, *FY 2004 Reporting Instructions for the Federal Information Security Management Act* (2004).

The document review process included Corporation:

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

An internal penetration test was conducted to evaluate security aspects of the Corporation's servers, printers, workstations, and network infrastructure from inside the Corporation firewall. The test was performed from inside the Corporation security perimeter in close coordination with the Deputy CIO and Network Administrator. Network vulnerability scans were performed using the System Administrator's Integrated Network Tool (SAINT®).

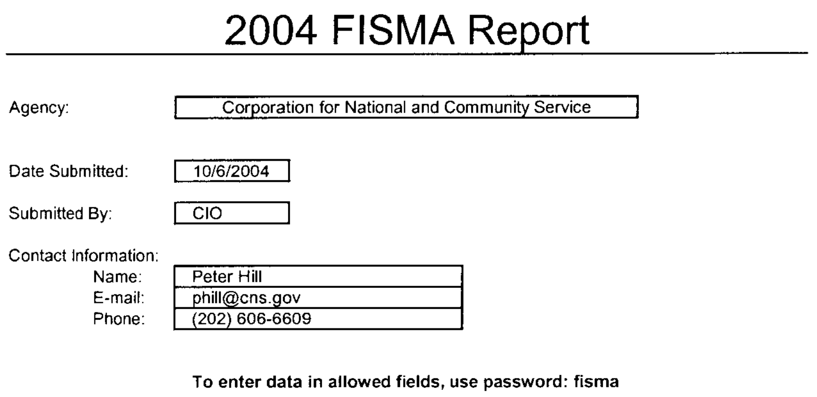
An external penetration test was conducted to evaluate security aspects of the Corporation's firewall. The test was performed from outside the Corporation's security perimeter (i.e., from the Internet). Network vulnerability scans were performed using SAINT®.

Analyses were performed in accordance with guidance from the following:

- 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 standards; and
- Corporation OIG guidance.

The independent evaluation was conducted on-site at Corporation Headquarters, 1201 New York Avenue, NW, Washington, DC 20525, between May 5, 2004, and September 3, 2004. Evaluators were Karen Frey, Jane Laroussi, Anthony Van Dyck, and Diane Reilly from Richard S. Carson & Associates, Inc., 4720 Montgomery Lane, Suite 800, Bethesda, MD 20814.

OFFICE OF MANAGEMENT AND BUDGET (OMB) 2004 FISMA REPORT



2004 FISMA Report

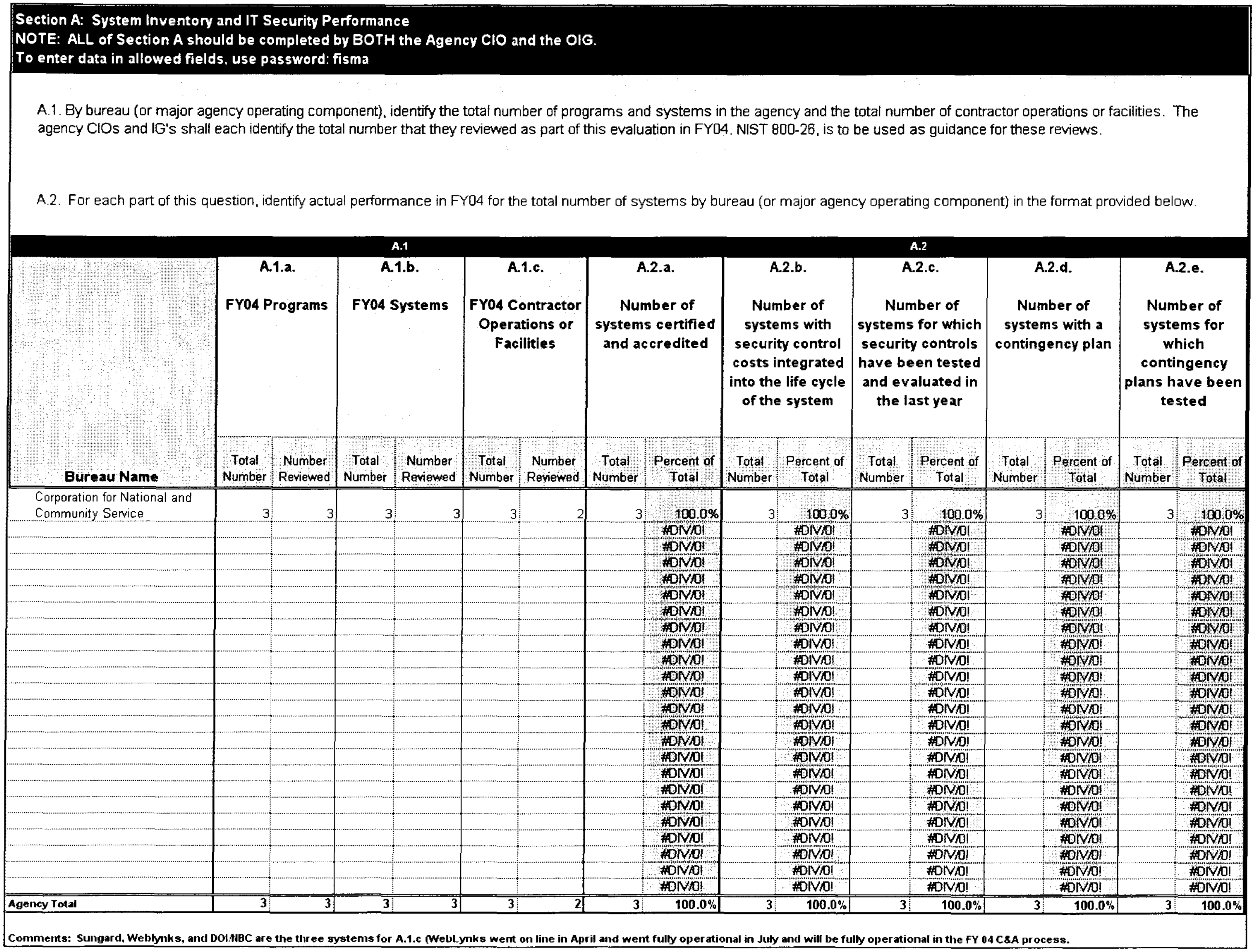
Agency: Corporation for National and Community Service

Date Submitted: 10/6/2004

Submitted By: CIO

Contact Information:
Name: Peter Hill
E-mail: phill@cns.gov
Phone: (202) 606-6609

To enter data in allowed fields, use password: fisma



Section A: System Inventory and IT Security Performance
NOTE: ALL of Section A should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

A.1. By bureau (or major agency operating component), identify the total number of programs and systems in the agency and the total number of contractor operations or facilities. The agency CIOs and IG's shall each identify the total number that they reviewed as part of this evaluation in FY04. NIST 800-26, is to be used as guidance for these reviews.

A.2. For each part of this question, identify actual performance in FY04 for the total number of systems by bureau (or major agency operating component) in the format provided below.

	A.1						A.2									
	A.1.a. **FY04 Programs**		**A.1.b.** **FY04 Systems**		**A.1.c.** **FY04 Contractor Operations or Facilities**		**A.2.a.** **Number of systems certified and accredited**		**A.2.b.** **Number of systems with security control costs integrated into the life cycle of the system**		**A.2.c.** **Number of systems for which security controls have been tested and evaluated in the last year**		**A.2.d.** **Number of systems with a contingency plan**		**A.2.e.** **Number of systems for which contingency plans have been tested**	
Bureau Name	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	Total Number	Percent of Total	Total Number	Percent of Total
Corporation for National and Community Service	3	3	3	3	3	2	3	100.0%	3	100.0%	3	100.0%	3	100.0%	3	100.0%
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
								#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!		#DIV/0!
Agency Total	3	3	3	3	3	2	3	100.0%	3	100.0%	3	100.0%	3	100.0%	3	100.0%

Comments: Sungard, Weblynks, and DOI/NBC are the three systems for A.1.c (WebLynks went on line in April and went fully operational in July and will be fully operational in the FY 04 C&A process.

A.3

A.3. 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 Comment area provided below.

Statement	Evaluation
a. Agency program officials and the agency CIO have used appropriate methods to ensure that contractor provided services or services provided by another agency for their program and systems are adequately secure and meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy.	Almost Always, or 96-100% of the time
b. The reviews of programs, systems, and contractor operations or facilities, identified above, were conducted using the NIST self-assessment guide, 800-26	Rarely, or 0-50% of the time
c. In instances where the NIST self-assessment guide was not used to conduct reviews, the alternative methodology used addressed all elements of the NIST guide.	Sometimes, or 51-70% of the time
d. The agency maintains an inventory of major IT systems and this inventory is updated at least annually.	Almost Always, or 96-100% of the time
e. The OIG was included in the development and verification of the agency's IT system inventory.	Almost Always, or 96-100% of the time
f. The OIG and the CIO agree on the total number of programs, systems, and contractor operations or facilities.	Almost Always, or 96-100% of the time
g. The agency CIO reviews and concurs with the major IT investment decisions of bureaus (or major operating components) within the agency.	Almost Always, or 96-100% of the time
Statement	**Yes or No**
h. The agency has begun to assess systems for e-authentication risk.	
i. The agency has appointed a senior agency information security officer that reports directly to the CIO.	

Comments: For h and i the system does not allow a visible user inputs. However the Corporation's response to both of these question is No.

Section B: Identification of Significant Deficiencies
NOTE: ALL of Section B should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

B.1. By bureau, identify all FY 04 significant deficiencies in policies, procedures, or practices required to be reported under existing law. Describe each on a separate row, and identify which are repeated from FY03. In addition, for each significant deficiency, indicate whether a POA&M has been developed. Insert rows as needed.

B.1.

	FY04 Significant Deficiencies			
Bureau Name	**Total Number**	**Number Repeated from FY03**	**Identify and Describe Each Significant Deficiency**	**POA&M developed? Yes or No**
Corporation for National and Community Services	1		No complete Annual Self-Assessments were completed for the Corporation's reported systems.	
Agency Total	1	0		

Comments:

Section C: OIG Assessment of the POA&M Process
NOTE: Section C should *ONLY* be completed by the OIG. The CIO should leave this section blank.
To enter data in allowed fields, use password: fisma

C.1. 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. This question is for IGs only. 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 Comment area provided below.

C.1	
Statement	**Evaluation**
a. Known IT security weaknesses, from all components, are incorporated into the POA&M.	Mostly, or 81-95% of the time
b. **Program officials** develop, implement, and manage POA&Ms for systems they own and operate (systems that support their program or programs) that have an IT security weakness.	Almost Always, or 96-100% of the time
c. Program officials report to the CIO on a regular basis (at least quarterly) on their remediation progress.	Almost Always, or 96-100% of the time
d. **CIO** develops, implements, and manages POA&Ms for every system they own and operate (a system that supports their program or programs) that has an IT security weakness.	Almost Always, or 96-100% of the time
e. CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	Almost Always, or 96-100% of the time
f. The POA&M is the authoritative agency **and** IG management tool to identify and monitor agency actions for correcting information and IT security weaknesses.	Almost Always, or 96-100% of the time
g. System-level POA&Ms are tied directly to the system budget request through the IT business case as required in OMB budget guidance (Circular A-11).	Almost Always, or 96-100% of the time
h. OIG has access to POA&Ms as requested.	Almost Always, or 96-100% of the time
i. OIG findings are incorporated into the POA&M process.	Almost Always, or 96-100% of the time
j. POA&M process prioritizes IT security weaknesses to help ensure that significant IT security weaknesses are addressed in a timely manner and receive appropriate resources.	Almost Always, or 96-100% of the time

Comments:

C.1 OIG Assessment of the Certification and Accreditation Process

Section C should only be completed by the OIG. OMB is requesting IGs to assess the agency's certification and accreditation process in order to provide a qualitative assessment of this critical activity. This assessment should consider the quality of the Agency's certification and accreditation process. Any new certification and accreditation work initiated after completion of NIST Special Publication 800-37 should be consistent with NIST Special Publication 800-37. This includes use of the FIPS 199, "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. Earlier NIST guidance is applicable to any certification and accreditation work completed or initiated before finalization of NIST Special Publication 800-37. Agencies were not expected to use NIST Special Publication 800-37 as guidance before it became final.

Statement	Evaluation
Assess the overall quality of the Agency's certification and accreditation process. **Comments:**	Satisfactory

Section D

NOTE: ALL of Section D should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

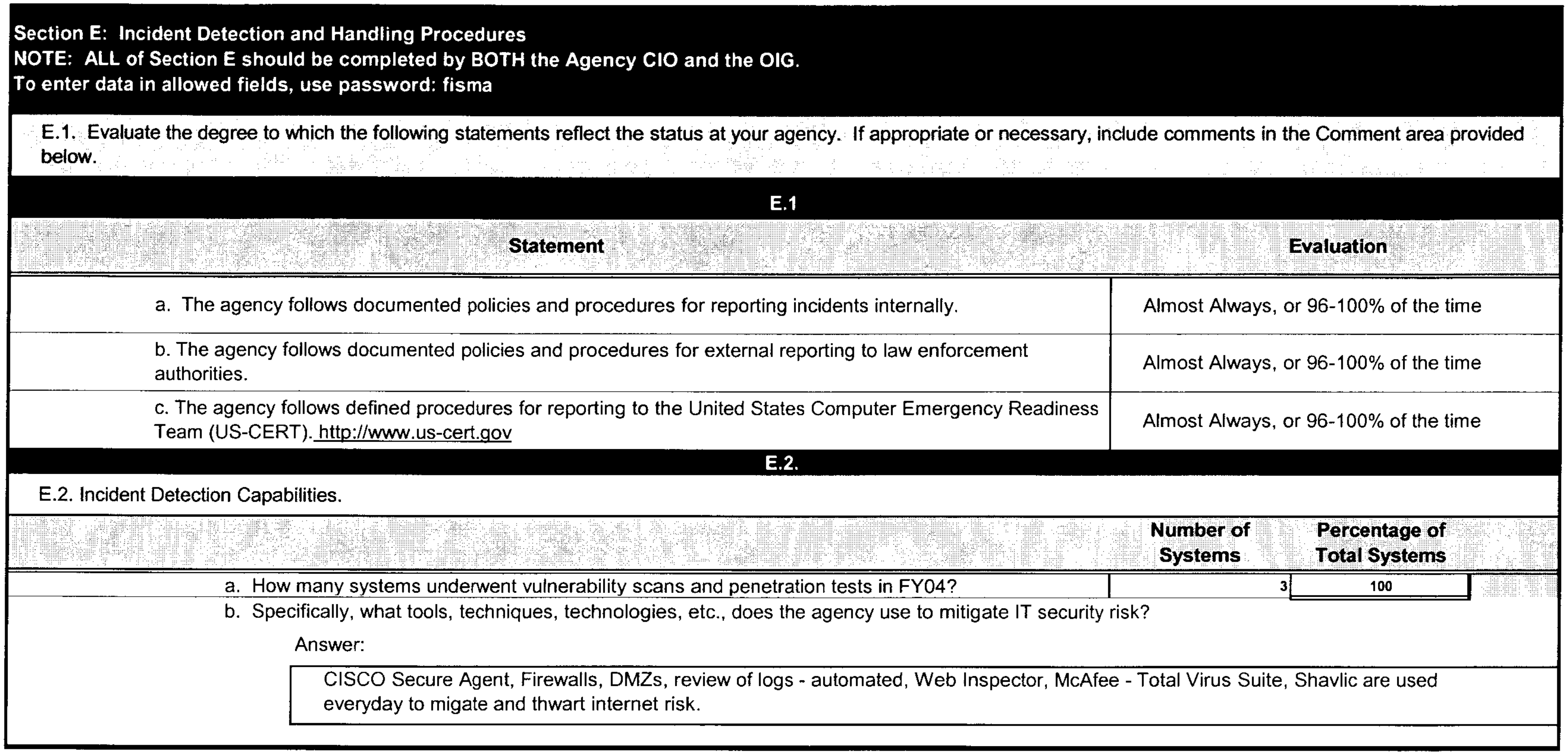
D.1. First, answer D.1. If the answer is yes, then proceed. If no, then skip to Section E. For D.1.a-f, identify whether agencywide security configuration requirements address each listed application or operating system (Yes, No, or Not Applicable), and then evaluate the degree to which these configurations are implemented on applicable systems. **For example:** If your agency has a total of 200 systems, and 100 of those systems are running Windows 2000, the universe for evaluation of degree would be 100 systems. If 61 of those 100 systems follow configuration requirement policies, and the configuration controls are implemented, the answer would reflect "yes" and "51-70%". If appropriate or necessary, include comments in the Comment area provided below.

D.2. Answer Yes or No, and then evaluate the degree to which the configuration requirements address the patching of security vulnerabilities. If appropriate or necessary, include comments in the Comment area provided below.

D.1. & D.2.

	Yes, No, or N/A	**Evaluation**
D.1. Has the CIO implemented agencywide policies that require detailed specific security configurations and what is the degree by which the configurations are implemented?		
a. Windows XP Professional	Yes	Almost Always, or 96-100% of the time
b. Windows NT	Yes	Almost Always, or 96-100% of the time
c. Windows 2000 Professional	Yes	Almost Always, or 96-100% of the time
d. Windows 2000	Yes	Almost Always, or 96-100% of the time
e. Windows 2000 Server	Yes	Almost Always, or 96-100% of the time
f. Windows 2003 Server	No	Rarely, or 0-50% of the time
g. Solaris	No	Rarely, or 0-50% of the time
h. HP-UX	No	Rarely, or 0-50% of the time
i. Linux	No	Rarely, or 0-50% of the time
j. Cisco Router IOS	Yes	Almost Always, or 96-100% of the time
k. Oracle	Yes	Almost Always, or 96-100% of the time
l. Other. Specify:	Yes	Almost Always, or 96-100% of the time
	Yes or No	**Evaluation**
D.2. Do the configuration requirements implemented above in D.1.a-f., address patching of security vulnerabilities?	Yes	

Comments:



Section E: Incident Detection and Handling Procedures
NOTE: ALL of Section E should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

E.1. Evaluate the degree to which the following statements reflect the status at your agency. If appropriate or necessary, include comments in the Comment area provided below.

E.1

Statement	Evaluation
a. The agency follows documented policies and procedures for reporting incidents internally.	Almost Always, or 96-100% of the time
b. The agency follows documented policies and procedures for external reporting to law enforcement authorities.	Almost Always, or 96-100% of the time
c. The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov	Almost Always, or 96-100% of the time

E.2.

E.2. Incident Detection Capabilities.

	Number of Systems	Percentage of Total Systems
a. How many systems underwent vulnerability scans and penetration tests in FY04?	3	100

b. Specifically, what tools, techniques, technologies, etc., does the agency use to mitigate IT security risk?

Answer:

CISCO Secure Agent, Firewalls, DMZs, review of logs - automated, Web Inspector, McAfee - Total Virus Suite, Shavlic are used everyday to migate and thwart internet risk.

Comments:

Section F: Incident Reporting and Analysis
NOTE: ALL of Section F should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

F.1. For each category of incident listed: identify the total number of successful incidents in FY04, 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 VII, "Other". If appropriate or necessary, include comments in the Comment area provided below.

F.2. Identify the **number of systems** affected by each category of incident in FY04. If appropriate or necessary, include comments in the Comment area provided below.

F.1., F.2. & F.3.						
	F.1. **Number of Incidents, by category:**			**F.2.** **Number of systems affected, by category, on:**		
	F.1.a **Reported internally**	**F.1.b.** **Reported to US CERT**	**F.1.c.** **Reported to law enforcement**	**F.2.a.** **Systems with complete and up to-date C&A**	**F.2.b.** **Systems without complete and up to-date C&A**	**F.2.c.** **How many successful incidents occurred for known vulnerabilities for which a patch was available?**
	Number of Incidents	**Number of Incidents**	**Number of Incidents**	**Number of Systems Affected**	**Number of Systems Affected**	**Number of Systems Affected**
I. Root Compromise	0	0	0	0	0	0
II. User Compromise	0	0	0	0	0	0
III. Denial of Service Attack	1	1	0	1	0	0
IV. Website Defacement	0	0	0	0	0	0
V. Detection of Malicious Logic	0	0	0	0	0	0
VI. Sucessful Virus/worm Introduction	4	0	0	4	0	2
VII. Other	0	0	0	0	0	0
Totals:	5	1	0	5	0	2

Comments: 2 user workstations were compromised.

DOS attack was self-inflected due to automatic cleansing of e-mail msgs and physical limitations of Exchanges 5.5 .... Occurred on Sept 08, 2003

F.2.c We had two sytems that got infected before McAfee published the Virus updates.

Section G: Training
NOTE: ALL of Section G should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

G.1. Has the agency CIO ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities? If appropriate or necessary, include comments in the Comment area provided below.

G.1.

G.1.a. Total number of employees in FY04	G.1.b. Employees that received IT security awareness training in FY04, as described in NIST Special Publication 800-50		G.1.c. Total number of employees with significant IT security responsibilities	G.1.d. Employees with significant security responsibilities that received specialized training, as described in NIST Special Publications 800-50 and 800-16		G.1.e. Briefly describe training provided	G.1.f. Total costs for providing IT security training in FY04 (in $'s)
	Number	Percentage		Number	Percentage		
637	637	1	5	1	0.2	Discussion of Sensitive information and its protection and all Corporation security policies.	$10,000

G.2.

	Yes or No	
a. 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	

Comments: P2P is not enabled. Web Inspector is ran to detect for the prescence of of P2P software. Firewall is set to block P2P traffic.

AGENCY RESPONSE TO FY 2004 INDEPENDENT EVALUATION REPORT

Response to OIG Report Number 04-24, CNS 2004 FISMA Independent Evaluation Report

Finding
The Corporation's major applications and general support systems security have not undergone testing and evaluation in the past 12 months, resulting in non-compliance with FISMA in the area of annual testing and evaluation.

Response:
The Corporation does not agree with this finding. We would like to direct your attention to the NIST ASSET tool reports that were completed for the Corporation's systems in September 2003 which were provided under separate cover. Additionally, it should be noted that regular testing and evaluation for major applications and general support systems is ongoing, as is regular vulnerability scanning and patch management implementation. The Corporation performs weekly penetration testing using Qualys services. Enterprise virus scanning is conducted at both the workstation and server level with hourly updates. Firewall and email monitoring occur and reverse lookups are performed before allowing web access or email to be received. Internally, the Corporation runs Cisco's IDS to monitor all core traffic and capture all suspicious activities. The Corporation has a detailed patch application process which makes use of Shavlik in a methodology that minimizes the exposure of critical systems. Additionally, all software modifications go through a rigorous review and implementation process that results in both system and user acceptance testing. The regular system monitoring and testing that we perform are designed to ensure that new threats and vulnerabilities do not go undetected.

During the last two fiscal years the Corporation's systems have been reviewed as part of 5 separate audits which have resulted in finding no significant security deficiencies. While these do not constitute C &A's or self assessment they are done annually and should identify significant security problems with the systems. Therefore we disagree that this finding is a significant deficiency. According to OMB a significant deficiency is:

"**Significant Deficiency** – is a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems, that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operation, or assets. In this context, the risk is great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken."

Additionally the OMB Memorandum cites, as a specific example, reliance on older data as not creating the type of risk rising to the level of a significant deficiency.

However, we do agree that not all the documentation regarding the system monitoring, testing and configuration management activities has been adequately maintained in support of the ASSET tool and this documentation will to be strengthened. The annual asset tool results were produced in accordance with NIST SP 800-26. We did provide a list of items that were identified in the ASSET tool evaluation that we addressed since the evaluation. In our view, the shortcomings in the supporting documentation do not impede the Corporation's ability to complete its mission, do not expose the Corporation to a significant IT risk, nor do they seriously jeopardize the Corporation's security program. It is a reportable condition that will be resolved by November 2004 with the completion of Certification & Accreditations of all systems. In addition we are in the process of completing this year's ASSET tool evaluation that will include much better documentation of the review process.

Finding
While the Corporation has established a single, agency-wide Plan of Action and Milestones (POA&M), as recommended in the FISMA Review for 2003, the POA&M has not been maintained in accordance with OMB guidance, which requires a baseline POA&M.

Response
The Corporation does maintain a POA&M, however it made an administrative error in not maintaining the original milestone dates on the POA&M. The Corporation has since marked the June 15th FISMA quarterly report as its baseline POA&M. The September 15th quarterly report confirms this. We consider this item now closed.

<u>Risk Assessment Section</u>

Finding
Risk assessments do not identify the names of participants involved in developing the risk assessments.

Recommendation
Add the names and titles of participants to Section II, Risk Assessment Approach, for each risk assessment.

Response
The Corporation will make this correction in the risk assessments currently underway, which are being conducted as part of the systems re-certification effort on the Network, Momentum, and e-SPAN scheduled to be completed by November 2004.

<u>Security Policies and Procedures</u>

Finding
The current System Development Life Cycle (SDLC) does not include a methodology to dispose of hardware or software.

Recommendation
Incorporate a disposal phase into the SDLC documentation in accordance with NIST SP 800-64.

Complete the approval process for the new SDLC s soon as possible.

Response
The Corporation has included additional sections on commercial off the shelf software and disposal phase to the SDLC. OIT has resubmitted the SDLC policy and it is in the process of being approved by Corporation management. That approval is expected to be completed by the end of October 2004.

System Security Plans
Finding
The Corporation Network system security plan does not address previously conducted control reviews. This omission can lead to duplication of effort and waste of time and money.

Recommendation
Update the network system security plan to reflect previously conducted security control reviews.

Response
The Corporation network is being re-certified and previous reviews will be included in the system security plan per NIST 800-18.

Finding
While conducting site surveys, a number of information security infractions of the policy (policy #501) were noted.

Recommendation:
Draw attention to the Corporation Policy #501 during the Corporation security awareness program.

Response:
The Corporation has issued an all hands e-mail calling attention to the policy #501 dealing with information security and protection. The Corporation has incorporated an information security section in the new employee orientation class. The first of these classes was held during New Employee Orientation on September 15, 2004. Finally, the Corporation will review the on-line security awareness course taken annually by all employees and make any appropriate changes to ensure information security practices are included.

Finding

A summary of major application security plans is not included in the Corporation's information technology (IT) Strategic Plan. This Finding was also cited in the FY 2003 FISMA report.

Recommendation

Include system security plan summaries in the IT Strategic Plan.

Response:

The Corporation will include the summaries in its IT strategic plan, due for completion by March, 2005.

Annual Testing and Evaluation

Finding

The Corporation's major applications and general support system security have not undergone testing and evaluation in the past 12 months, resulting in noncompliance with FISMA in the area of annual testing and evaluation. This is considered a significant deficiency.

Recommendation

Conduct annual self-assessments in accordance with NIST SP 800-2.

Response:

See the Corporation's response to this finding on page 1.

Finding

"...the Corporation's stated practice is to perform annual C&A's in lieu of self assessments....No C&A's were completed in the last 12 months.

Recommendation:

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

Response

The Corporation performed its 2003 reviews using the NIST ASSET tool believing this to be adequate to meet the full requirement. It should be noted that at no time were any of the Corporation's systems not covered by a signed C&A. While it is the Corporation's intent to perform yearly C&A's a policy will be developed to provide the necessary flexibility to meet unexpected testing requirements and maintain continuity in the assessment process. Therefore, the Corporation is developing a certification and accreditation program policy that will include FISMA compliant annual testing procedures and requirements. The expected completion date is November 2004.

Corrective Action Process

Finding

Details from the various audits, C&A's, and independent evaluations are not being recorded in the POA&M, causing relevant information to be overlooked in the tracking process.

Recommendation

Improve the current single, agency-wide POA&M process by tracking all reported weaknesses until closed.

Response:

The Corporation is taking steps to ensure all security related findings are duly entered into the agency-wide POA&M.

Finding

The POA&M has not been maintained in accordance with OMB guidance that requires a base line POA&M.

Recommendation:

Maintain the POA&M in accordance with OMB submission guidelines requiring that data in columns 1, 4, 5, 7 remain fixed, to serve as the baseline for subsequent quarterly updates.

Response

See the Corporation's response to this finding on page 2.

Continuity of Operations

Finding

The Disaster Recovery plan, dated August 2003, is well-written and generally adheres to NIST guidelines. However, several discrepancies were noted. ...Disaster recovery team responsibilities were listed as "TBD at a later date", Windows NT is the stated operating system but the Corporation uses Windows 2000 platform. The Corporation organization chart remains "TBD".

The Corporation Network Contingency Plan, dated August 2001, does not fully follow NIST guidelines.

Recommendation

Revise and Update the Corporation disaster recovery plan and contingency plan as necessary to meet NIST SP 800-34 guidelines.

Response

The Corporation disagrees with this finding because the reviewed documentation was correct for the time period during which the test was conducted (September, 2003). The Corporation is in the process of updating the DRP as part of OIT's yearly testing which is scheduled to be completed by September 30, 2004. The contingency plans for the organization and its systems are being updated as well and are expected to be completed in December 2004.

Finding

A limited contingency plan test was conducted at Corporation Headquarters in September 2003, but the alternate disaster recovery site was not tested. Test results were not retained, however.

Recommendation

Retain continuity of operations test results for examination by future audits, reviews, and independent evaluations.

Response

The Corporation acknowledges the testing results need to be maintained in a more formal manner and is taking steps to establish a testing results documentation library within OIT. This will be completed by in December, 2004.

Recommendation

Formally document that the alternate disaster recovery site for e-Grants was not being tested, and issue a letter of acceptance of risk for senior management approval.

Response

The Corporation will issue the risk acceptance in a formal letter to be signed by the appropriate officials and placed in the system accreditation files. This will also be included in the September 2004, Disaster Recovery testing acceptance documentation.

Configuration Management

Finding

Configuration Management (CM) of Corporation systems and assets is performed in an effective manner, but the process has not been formalized.

Recommendation

Develop a configuration management plan and obtain senior management approval.

Response

The Corporation is formalizing its CM process and expects to complete the first draft document by November 2004.