**OFFICE OF INSPECTOR GENERAL**
**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE**

# Independent Audit Report of Office of Inspector General Review of Corporation for National and Community Service Implementation of the Federal Information Security Management Act For Fiscal Year 2003

**OIG Audit Report Number 03-25**
**August 21, 2003**

Prepared by:

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

**This report was issued to Corporation management on September 18, 2003. Under the laws and regulations governing audit follow up, the Corporation must make final management decisions on the report's findings and recommendations not later than March 18, 2004, and complete its corrective actions by September 18, 2004. Consequently, the report findings do not necessarily represent the final resolution of the issues presented.**

## BACKGROUND

Richard S. Carson & Associates, Inc. (Carson Associates), on behalf of the Office of Inspector General (OIG) of the Corporation for National and Community Service (CNCS), completed this Independent Audit Report. The Independent Audit Report provides findings and conclusions and, when applicable, identifies problem areas and makes recommendations for resolution.

On December 17, 2002, President George W. Bush signed into law the E-Government Act of 2002 (Pub. L. No. 107-347), which includes Title III, the Federal Information Security Management Act of 2002 (FISMA). The FISMA permanently reauthorized the framework laid out in the Government Information Security Reform Act of 2000 (GISRA), which expired in November 2002. The FISMA outlines the information security management requirements for agencies, including the requirement for annual review and independent assessment by agency inspectors general. In addition, FISMA includes new provisions aimed at further strengthening the security of the Federal government's information and information systems, such as the development of minimum standards for agency systems. The annual assessments provide agencies with the information needed to determine the effectiveness of overall security programs and to develop strategies and best practices for improving information security.

The independent audit comprises four elements: evaluation of CNCS's information security program, evaluation of CNCS progress towards correcting weaknesses addressed within the 2002 Plan of Action and Milestones (POA&Ms), review of Corporation self-assessments and verification and testing of information security controls for four representative information systems. The results of the independent audit address the problems identified during the evaluation. The major findings from the report are summarized in the Results in Brief.

## PURPOSE

The objectives of the independent audit of CNCS's information security program were to:

- Test the effectiveness of information security policies, procedures and practices of a representative subset of the agency's information systems;
- Assess compliance with FISMA and related information security policies, procedures, standards and guidelines; and
- Conduct follow-up assessment of agency progress in correcting weaknesses identified in prior GISRA/FISMA evaluations, including those weaknesses listed in the Fiscal Year (FY) 2002 POA&M.

## RESULTS IN BRIEF

CNCS has taken a number of steps during the past year to enhance its security program and address issues identified in the 2002 GISRA report. These enhancements are as follows:

- Hardware and software have been acquired and installed to provide Continuity of Operations (COOP) for the e-Grants system.

- The COOP has been successfully tested for e-Grants, with full capability anticipated by the end of this fiscal year.

- Certification and Accreditations (C&As) were completed for all major applications (MA) during this reporting period.

- Improvements have been made to the test planning and execution process. Efforts are ongoing to integrate these improvements into the formal Systems Development Lifecycle (SDLC) methodology.

- CNCS maintains a very effective security awareness program; all employees and contractors (requiring system access) undergo annual security awareness training.

- Configuration Management (CM) policies include extensive work in the tracking of hardware inventory and software licensing, as well as the use of automation tools to track system level configurations for desktop deployment and configuration control.

Notwithstanding the improvements stated above, some areas showed little progress toward remediation and/or did not adhere to Office of Management and Budget (OMB) A-130 guidance. These areas were identified as problems.

- The lack of system-level rules of behavior for the Electronic-System for Program Agreements and National Service Participants (E-SPAN) and Electronic-Grants (e-Grants) were identified as a weakness in last year's GISRA assessment, but have not been documented or addressed to date. While there are a variety of policies and procedures for system users and many cover "rules" that affect applicable systems, Program Officials have not defined system-specific rules as required by OMB A-130.

- The 2002 GISRA report stated that a summary of major system security plans was not included in the Corporation's Information Management (IM) Strategic Plan. This item is identified in the agency-wide POA&M but, to date, has not been included in the IM Strategic Plan. However, during an August 2003 interview with the Deputy Chief Information Officer (Deputy CIO), it was determined that this weakness is now being addressed and should be resolved upon publication of the revised plan this year.

- The Corporation has a stated policy to perform complete C&A processes for all major systems each year (versus every three years or whenever a major system change occurs), rather than performing annual tests and evaluations as defined in OMB A-130. However, there is no documented policy within CNCS stating annual System Test and Evaluation (ST&E) and risk-assessment processes will be accomplished as a part of C&A.

- The Corporation's corrective action process needs to be improved to ensure that all Information Technology (IT) security weaknesses are identified on system-level POA&Ms and that the Program Officials and the OIG track and support resolution of these actions in a pro-active, collaborative way. The Corporation's Deputy CIO and OIG maintain a variety of tracking systems and maintain their own processes. However, the POA&M process, as described by OMB A-130 and recent FISMA reporting guidance issued August 6, 2003, is not the Corporation's authoritative management tool for tracking IT security weaknesses.

- The Corporation identifies their major systems in a variety of methods, such as Exhibit 300s, Security Plans and the IM Strategic Plan. However, there is no single source for maintaining the Corporation's inventory of major systems and their inter-connections

with other systems. The resulting condition is a lack of reconciliation between documents and reporting methods concerning the official list of major systems within CNCS.

## RECOMMENDATIONS

Based on these findings, the audit team has made a number of recommendations to strengthen CNCS's security program. The list of recommendations made to CNCS is consolidated at page 11.

## AGENCY COMMENTS

At an exit conference held on August 21, 2003, CNCS officials generally agreed with the findings. The comments provided by CNCS and OIG officials on August 26, 2003, have been incorporated in the report where appropriate.

Upon review of the draft report, CNCS officials provided a formal response to the report and recommendations contained therein. This response is provided at Appendix C.

## ABBREVIATIONS AND ACRONYMS

| | |
|---|---|
| AIS | Automated Information Systems |
| BCCP | Business Continuity/Contingency Plan |
| 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 |
| CNCS | Corporation for National and Community Service |
| COOP | Continuity of Operations Plan |
| COTS | Commercial Off-the-Shelf Software |
| DMZ | Demilitarized Zone |
| DNS | Domain Name Service |
| DOI | Department of Interior |
| 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 |
| FedCIRC | Federal Computer Incident Response Center |
| FISMA | Federal Information Security Management Act |
| FY | Fiscal Year |
| GAGAS | Generally Accepted Government Auditing Standards |
| GAO | U.S. General Accounting Office |
| GISRA | Government Information Security Reform Act |
| GSS | General Support Systems |
| IG | Inspector General |
| ISACA | Information Systems Audit & Control Association |
| ISSO | Information Systems Security Officer |
| IM | Information Management |
| IP | Internet Protocol |
| IRM | Information Resource Management |
| IT | Information Technology |
| LAN | Local Area Network |
| MA | Major Application |
| MOA | Memorandum of Agreement |
| MOU | Memorandum of Understanding |
| 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 |
| OS | Operating System |
| OWA | Outlook Web Access |
| POA&M | Plan of Action and Milestones |
| RPC | Remote Procedure Call |
| SAINT™ | System Administrator's Integrated Network Tool |
| SAS 70 | Statement on Auditing Standards (SAS) No. 70 |
| SDLC | Systems Development Lifecycle (SDLC) |
| SIR | Security Incident Report |
| SLA | Service Level Agreement |
| SNMP | Simple Network Management Protocol |
| SP | Special Publication |
| ST&E | System Test and Evaluation |
| WBRS | Web-based Reporting System |

# TABLE OF CONTENTS

## Background

Richard S. Carson & Associates, Inc. (Carson Associates), on behalf of the Office of Inspector General (OIG) of the Corporation for National and Community Service (CNCS), completed this Independent Audit Report. The Independent Audit Report provides findings and conclusions and, when applicable, identifies problem areas and makes recommendations for resolution.

On December 17, 2002, President George W. Bush signed into law the E-Government Act of 2002 (Pub. L. No. 107-347), which includes Title III, the Federal Information Security Management Act of 2002 (FISMA). The FISMA permanently reauthorized the framework laid out in the Government Information Security Reform Act of 2000 (GISRA), which expired in November 2002. The FISMA outlines the information security management requirements for agencies, including the requirement for annual review and independent assessment by agency inspectors general. In addition, FISMA includes new provisions aimed at further strengthening the security of the Federal government's information and information systems, such as the development of minimum standards for agency systems. The annual assessments provide agencies with the information needed to determine the effectiveness of overall security programs and to develop strategies and best practices for improving information security.

The independent audit comprises four elements: evaluation of CNCS's information security program, evaluation of CNCS progress towards correcting weaknesses addressed within the 2002 Plan of Action and Milestones (POA&Ms), review of Corporation self-assessments, and verification and testing of information security controls for four representative information systems. The results of the independent audit are presented in a separate Independent Audit Report that presents a number of recommendations to address the problems identified during the evaluation. The major findings from the report are summarized in the Results in Brief.

## Purpose

The objectives of the independent audit of CNCS's information security program were to:

- Test the effectiveness of information security policies, procedures and practices of a representative subset of the agency's information systems;
- Assess compliance with FISMA and related information security policies, procedures, standards and guidelines; and
- Conduct follow-up assessment of agency progress in correcting weaknesses identified in prior GISRA/FISMA evaluations, including those weaknesses listed in the fiscal year 2002 POA&M.

This audit report is a stand-alone document and also serves as the authoritative source for the Executive Summary to the Office of Management and Budget.

The audit was conducted in accordance with Generally Accepted Government Auditing Standards. All applicable standards were followed.

## Independent Audit

The information contained in this section provides the findings from research, analysis and assessment of the Corporation's information security program. Compliance with security standards prescribed by OMB, the National Institute of Standards and Technology (NIST) and related authoritative policies, procedures, standards and guidelines (criteria), where applicable, will be cited when describing a specific finding (condition). When appropriate, root cause and affect will be included in the discussion. Lastly,

recommendations will also be made for any weaknesses and/or deficiencies noted. These recommendations are intended to assist CNCS in determining the corrective action needed.

## Agency Risk Assessments

### Conclusions and Findings

**The Corporation's major system security plans have all undergone risk assessments, as part of their Certification and Accreditation (C&A) processes, within the last year.** OMB A-130 requires that Federal agencies use a risk assessment process when developing security plans. Within CNCS, OMB A-130 was followed. *NIST Security Self-Assessment Guide for Information Technology Systems,* Special Publication (SP) 800-26, was used to develop security plans for their major systems and to conduct the risk assessments. Any risks identified were evaluated by the Information System Security Office (ISSO) and were addressed in the cover letter to the Deputy CIO, as the certifying authority. As a result of these assessments, Program Officials are able to determine the security of their systems and address any weaknesses or vulnerabilities before they can be exploited.

### Recommendations

- Based on findings associated with agency risk assessments, we recommend that CNCS continue to conduct annual risk assessments in accordance with their well-established organizational practices.

## Security Policies and Procedures

### Conclusions and Findings

**The Corporation has a very comprehensive library of policies and procedures available to their staff through their intranet.** For example, policies include guidelines for obtaining accounts to the network, obtaining security awareness training, using Internet and e-mail systems, protecting and handling sensitive information and responding to incidents. Subject areas are comprehensive, covering network system and agency-wide security topics. In addition to security policies, the library includes the Business Contingency/Continuity of Operations Plan (BCCP) for the network and a Continuity of Operations Plan (COOP) for each of the major systems. These systems define the roles and responsibilities for applicable staff members and contractors, in order to execute the plans in the event of system failure

**The current SDLC does not include methodologies to support findings from the latest risk assessments concerning test procedures, test plans and documented test results.** Not having a defined test methodology has resulted in many test items, risk-assessment findings and control test results not being tracked for analysis and resolution. OMB A-130 requires that agency heads take an active role in ensuring that security practices are followed throughout the systems' lifecycles. Within CNCS, the Deputy CIO has been an active participant in the development of the Systems Development Lifecycle (SDLC) used by the agency for application (system) development. To improve the test phase of the lifecycle, the Deputy CIO and system owners have recently collaborated to develop a process for test plan development and execution, including roles and responsibilities for the technical staff and end users. This material, while not fully integrated into the SDLC document, shows good progress toward achieving full integration of testing into the SDLC methodology.

**The current SDLC does not contain a methodology for evaluating and integrating Commercial Off-the-Self (COTS) products into CNCS's automated systems.** OMB criteria calls for ensuring security

practices are followed throughout the lifecycle. In today's computing environment, many agency systems contain pre-packaged products that can offer advanced capabilities without extensive customization by the technical staff. However, while the capabilities are not "developed" by the agency, the product is being integrated into the collective architecture, thus having a major impact upon the security configurations and practices in place. Therefore, COTS products should be addressed in the agency's SDLC documentation.

### Recommendations

Based on findings associated with security policies and procedures, we recommend that CNCS take the following actions to resolve SDLC weaknesses.

- Include test provisions in the SDLC.
- Include COTS evaluation provisions in the SDLC.

## System Security Plans

### Conclusions and Findings

**At the system level, the Electronic-System for Program Agreements and National Service Participants (E-SPAN) and Electronic-Grants (e-Grants) Application Security Plans do not contain system-specific rules of behavior for all individuals with access to the systems.** OMB A-130 [Appendix III, A(3)(b)(2)(a)] requires that agencies "establish a set of rules concerning the use of and behavior within the application." 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 effects of not having these rules can be numerous. In the case of E-SPAN and e-Grants, end users may not be aware of application-specific data sensitivities or be aware of key personnel that are responsible for release of grant data through the system. In addition, if there are any responsibilities that are shared between functional area experts and the technical staff, there may be confusion or misunderstanding concerning the lines of responsibility.

**A summary of major application security plans is not included in the Corporation's Information Management (IM) Strategic Plan.** This is a repeat finding, also identified during the 2002 GISRA report and currently documented and tracked on the agency-wide POA&M. OMB A-130 guidance [Appendix III, (A)(3)(a)(2)] 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)." In addition to non-compliance with the referenced policies, the effect on the agency's security program is two-fold. First, senior agency officials will not have the strategic security profile available to them, thus impacting security awareness concerning major applications at agency head level. Second, agency officials responsible for developing the strategic plan will not have system security information available to relate security issues to long-range budget and IT capital planning.

### Recommendations

Based on findings associated with security policies and procedures, we recommend that CNCS make policy and procedure enhancements as follow:

- Develop E-SPAN and e-Grants rules of behavior.
- Include system security plan summaries into the IM Strategic Plan.

## Security Awareness and Training

### Conclusions and Findings

**CNCS maintains a very effective security awareness program, ensuring all employees and contractors (with system access) undergo annual security awareness training.** OMB A-130 requires that "agencies provide security awareness training for all employees (ref: 2003 FISMA Guidance, p34)." Within CNCS, this program is very comprehensive and well maintained in accordance with OMB guidelines. The Deputy CIO and the ISSO take an active role in maintaining the security awareness of both the end users and technical staff that supports the Corporation. The ISSO maintains a database of all user security awareness training activity and proactively reminds users whenever their annual training is required. Corporate policies contain provisions for training prior to obtaining accounts and gaining access to the network, applications and sensitive information, as well as provisions for when accounts will be inactivated and retired. Training material is conveniently available to the users in multiple ways, such as on-line training or classroom instruction. Additionally, documentation is available to users on-line on how to report security incidents and what their responsibilities are in those instances. Users are also provided with information from the ISSO and the Office of Information Technology (OIT) Help Desk regarding current security concerns, such as Federal Computer Incident Response Center (FedCIRC) virus alerts.

### Recommendations

- Based on findings associated with the agency's security awareness training program, we recommend that CNCS continue to capitalize on current security awareness training practices and procedures.

## Annual Testing and Evaluation

### Conclusions and Findings

**All major systems reviewed during the assessment had recent C&A packages that contained risk assessments and security controls testing results**. FISMA and OMB guidance requires that all agency systems be reviewed at least annually, and use the NIST SP 800-26 or an agency-developed methodology that includes all NIST SP 800-26 requirements. As required, CNCS conducts testing and evaluation in accordance with the provisions of the NIST self-assessment guide (SP 800-26) and uses the results as a basis for security plan development.

**CNCS performs annual C&As, in lieu of annual testing and evaluation; however, there is no documented policy to ensure compliance with the annual requirement.** OMB policy requires that systems undergo complete C&A and security control testing every three years, or whenever a major system change occurs. OMB requires that all major systems undergo annual testing and evaluation to ensure that system environments remain secure. The Corporation supports both requirements by

performing complete C&As for all major systems. No other risk assessments are performed by agency staff or contractors. The annual independent FISMA audit is the only exception. The practice of performing annual C&As to satisfy the requirement for annual risk assessment, testing and evaluation is not a documented Corporation policy. While this practice ensures CNCS compliance with OMB and NIST policy, the use of this undocumented procedure could result in failure to perform annual testing if system owners are not aware of this approach.

**The CNCS Corporation performs scans of their network to identify and mitigate possible vulnerabilities.**

Internal Scanning conducted by CNCS
The OIT staff utilizes specialized scanning software to perform detailed vulnerability scans of their architecture to identify such issues such as patch update requirements, open ports and services that are running on various servers, routers and workstations. These scans are executed routinely, but are also run after a change has been made to the architecture to ensure the configuration is secure and meets current CM requirements maintained for the network. OIT's methodology includes performing system changes and updates on a test platform and re-running applicable scans to validate changes, prior to deployment in the production environment.

Internal Scanning conducted by outside consultant
The OIG's independent FISMA evaluation included internal scanning. On August 6, 2003, an internal vulnerability assessment was conducted using the Security Administrator's Integrated Network Tool (SAINT™). SAINT™ analyzes the network signature of a given host, assesses the signature for probable vulnerabilities, ranks the vulnerabilities in terms of severity, reports the vulnerabilities and suggests a remedial course of action. Carson Associates worked with OIT to identify what hosts to scan. A full SAINT™ scan was conducted by attaching a laptop with the SAINT™ software installed on it to the CNCS network. Scan targets included central file servers and printers, a sample of service centers and state offices and the Corporation's Demilitarized Zone (DMZ) servers. Upon completion of the scans, the laptop was removed from the CNCS network and taken to the Carson Associates office in Bethesda, MD. There the data was analyzed and the results compiled for delivery to CNCS. All data and products were then delivered to CNCS and the data removed from the Carson Associates laptop. The detailed results from these scans were provided to CNCS with the results grouped in two views:

- Service Category (Critical Problems, Areas of Concern, Potential Problems, and Services that are not exploitable)

- Class (Web, Mail, File Transfer, Login/Shell, Print Services, Remote Procedure Call (RPC), Domain Name Service (DNS), Databases, Networking/Simple Network Mail Protocol (SNMP), Windows Operating System (OS), Passwords, and Other)

External scanning conducted by outside consultant
Carson Associates conducted external scans during the FISMA audit process. On August 20, 2003, an external assessment was performed using a variety of tools, including SAINT™, nslookup, whois, xprobe, nmap and nmblookup. In addition, several attempts were made to access specific ports and services identified by the SAINT™ scan. The external assessment was conducted "blind" (i.e., information from the previous internal assessment and other information previously learned about the CNCS network was not used during the external assessment). The external assessment was conducted using several steps:

- Identify CNCS IP Space – The first step was to identify the Internet Protocol (IP) space "owned" by CNCS. A combination of nslookup and the ARIN whois service were used to identify the target IP space.

- SAINT™ Scan – The next step was to perform a SAINT™ scan on the identified IP space. Attachment C contains the details from the SAINT™ scan.

- Nmap and xprobe Scans – After the SAINT™ scan, additional probes were performed using nmap and xprobe. The xprobe scans were useful in identifying possible operating system types for the seven hosts found by the SAINT™ scan.

- Outlook Web Access (OWA) Tests – Information gathered from the CNCS web site and the previous tests was used to gather possible OWA account names. Several attempts were made to try and access CNCS mailboxes.

- Port and Service Tests – Information gathered by the different scans was used to try and connect to various ports and use various services.

Upon completion of the scans, the data was analyzed and the results compiled for delivery to CNCS. The results of the analysis were provided to CNCS for their analysis and appropriate action.

### Recommendations

Based on findings associated with annual testing and evaluation, we recommend that CNCS take action as follows:

- Document the procedure for conducting annual tests and evaluation in a written policy.

- Review the results of the internal and external penetration tests conducted by Carson Associates during this evaluation, and resolve/mitigate vulnerabilities, as appropriate, to meet the security needs of the Corporation and its external customers.

## Corrective Action Process

### Conclusions and Findings

**CNCS maintains a single agency-wide POA&M and reports the status of actions on this POA&M to OMB on a quarterly basis.** The Deputy CIO maintains the agency-wide POA&M and tracks summary-level IT security weaknesses and security issues having significant financial resource implications. For example, findings concerning deficiencies in system-level documentation are aggregated and tracked as a single POA&M item, rather than stating distinct security weaknesses. The aggregate POA&M complies with OMB policy for agency head tracking and is used by the OIG during annual financial audits to evaluate items that may affect compliance with financial guidelines. However, greater granularity below summary level is needed for tracking IT security weaknesses identified through the various audit, assessment and testing processes. Implementation of a comprehensive tracking system, having both summary and system-level detail, would ensure multi-dimensional tracking by system owners, agency leadership and oversight bodies such as the OIG and auditors. Tracking should ensure a total integrated picture of IT security weaknesses, including both agency-wide and system-wide POA&Ms.

**Agency POA&Ms are not used as the authoritative management tool for tracking IT security weaknesses throughout the Corporation.** The 2003 FISMA Guidance (page 21) states that agency and system-level POA&Ms "should be the authoritative agency-wide management tool" for tracking corrective action items associated with security deficiencies. The Deputy CIO does maintain a tracking database for action items related to OIT activities. These action items are also tracked in various applications, such as the OIT Help Desk database, network action items, application "fix" lists and deployment lists. However, many of the IT security weaknesses and recommendations shown in risk assessments, GISRA/FISMA assessments and financial audits are not maintained in these tracking systems. Additionally, these tracking mechanisms are not used to track or produce system-level POA&Ms. The effect is that CNCS does maintain tracking capabilities to manage various types of action items (including many that are considered IT security weaknesses), but does not use POA&Ms as the authoritative tool as required by OMB. As a result, IT security weaknesses are not being tracked in a coordinated way by the various agency process owners and stakeholders. Utilizing the POA&M process as the predominant overarching tracking method would ensure FISMA compliance. It would also facilitate CNCS staff involvement in IT security weakness mitigation/resolution activities.

**Most IT security weaknesses and recommendations from the 2002 GISRA assessment, recent risk assessments and control tests are not tracked in the agency-wide POA&M or in system-level POA&Ms.** For example, the e-Grants C&A cover letter from the ISSO to the certifying authority states that "the overall risk exposure will remain low upon resolution and implementation of the recommendations listed in the document." However, prior audit findings are not listed in a POA&M or tracked in a manner that could be verified for status or resolution. NIST SP 800-26 states that the security certification package should contain the security plan, the security test and evaluation report and a POA&M list. FISMA guidance (August 6, 2003) also states that "an agency should develop a separate POA&M for every program and system for which weaknesses were identified in the FISMA reports, as well as those discovered during other reviews including General Accounting Office (GAO) audits, financial system audits, and critical infrastructure vulnerability assessments." Findings and recommendations are not tracked, managed, addressed or reported as required by FISMA. The possible impact is that IT security weaknesses and vulnerabilities may be overlooked or inadequately addressed and mitigated, resulting in unacceptable risk to the agency and related systems.

**CNCS functional leaders and the OIG are not involved in the POA&M resolution process.** Currently, the Deputy CIO acts on behalf of the agency head, CIO and functional area leaders to support the tracking of IT security weaknesses. The Deputy CIO also acts on behalf of the agency in the role of system owner for the Network, E-SPAN and e-Grants systems. Functional leaders are only involved in system-related activities to coordinate with the Deputy CIO and OIT staff to resolve issues that relate to the functionality and operations of their systems. The OIG is involved with the Corporation's IT activities during the annual financial audit process, independent FISMA assessment process and during major system design/re-design processes. As a result of the GISRA results from previous years, the Assistant Inspector General for Audit stated that "the OIG has taken steps to determine areas that should be included in the OIG's audit plans. For example, the OIG has completed additional network assessment testing and reported the results to Corporation Management in audit report 02-23". The OIG also maintains a tracking system to track OIG audit items. Recent FISMA guidance (August 6, 2003) has expanded the required role of the OIG and now requires "IGs to assess against specific criteria, whether the agency has developed, implemented, and manages an agency-wide POA&M process." Specifically, OMB Guidance (question a.4), asks whether "agency IGs are an integral part of the POA&M process and have access to agency POA&Ms." Notwithstanding OIG involvement during financial audits, this new guidance now requires OIGs to become more of an interactive participant in the POA&M process and to assess the effectiveness of the POA&M process in managing IT security weaknesses. In the current environment, the OIG and corporate system owners do not interact collaboratively within the framework of the agency security program.

Thus, there is a need for functional area leaders and the OIG to take a more proactive role in tracking and reporting POA&M items. Currently the Network, E-SPAN and eGrants are at the core of agency-owned systems and are under the central responsibility of the Deputy CIO. While the agency is of modest size (approximately 600 people) and the relatively small number of major systems and general support systems (less than six) may not require the separation of IT management duties, functional area leaders and the OIG still share responsibility for ensuring the protection of the systems and data upon which the agency depends to accomplish its mission.

### Recommendations

Based on findings associated with the corrective action process, recommend that CNCS expand upon the current single agency-wide POA&M to incorporate additional IT security improvements as follows:

- Track IT security weaknesses and recommendations in single, integrated process consisting of both agency-wide and system-level POA&Ms.
- Implement POA&Ms as the authoritative management tool for tracking IT security weaknesses.
- Increase CNCS functional leader and OIG involvement in the POA&M process.

## Security Incident Reporting

### Conclusions and Findings

**CNCS has developed and maintains an effective security incident reporting process that follows FedCIRC policies.** OMB A-130 requires that all agencies develop an incident response capability for their major applications and general support systems (2003 FISMA, p35). CNCS maintains a detailed policy available to all users through the CNCS intranet, providing thorough guidance concerning the Serious 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 there have been no incidents at CNCS headquarters, its Service Centers or State Offices that have required an SIR report to the FedCIRC.

Physical security incident reporting is the responsibility of Administrative Services, and are notified immediately if a physical security incident occurs. If the incident takes place within the headquarters facility, Administrative Services contacts the Federal Protective Services (FPS), who, in turn, responds to the incident. The Washington Metropolitan Police Department (MPD) is contacted for response to incidents outside the facility.

### Recommendations

- Based on findings associated with the security incident report (SIR) process, we recommend that CNCS continue to manage serious incident reporting as outlined in established agency policies and procedures.

## Continuity of Operations

### Conclusions and Findings

**All of the major applications reviewed during this assessment have undergone testing of their Continuity of Operations Plans (COOP) as part of the C&A processes.** The NIST *Contingency Planning Guide for Information Technology Systems* (SP 800-34), states that contingency plans should contain detailed records of system configurations in order to enhance system recovery capabilities. The 2002 GISRA Assessment Report stated that the e-Grants system COOP had been developed, but could not be tested due to the lack of hardware and software in the Disaster Recovery Site (DRS) to recover the DMZ. These resources were acquired and installed at the DRS, and the e-Grants COOP was tested in September 2002. All testing was successfully completed by October 2002. It was noted by the Deputy CIO that a portion of the e-Grants system had not been available for testing by the grantee, but will be available and tested in September 2003. The CNCS network has a current and tested BCCP that includes both COOP details to recover the technical environment and applications and contingencies to counter various failure scenarios. For example, a contingency exists for a Service Center losing connection with the CNCS network. In that instance, the center's capability is transitioned to an alternate site until the connection can be restored. In another example, if the dedicated connection to the Momentum system is interrupted, an alternate "fail-over" site exists to ensure continued operation.

**CNCS maintains a variety of mechanisms to ensure documented agreements between CNCS and outside agencies and contractors that maintain or own systems critical to CNCS operations.** NIST SP 800-34 states that "...memorandums of understanding (MOU), memorandum of agreement (MOA), or a Service Level Agreement (SLA) for an alternate site should be developed specific to the organization's needs and the partner organization's capabilities" (SP800-34, p22). MOUs represent partnerships between organizations to help them achieve mutual goals. CNCS has recently reviewed the Statement on Auditing Standards No. 70 (SAS 70) reports on the Department of Interior's National Business Center (NBC) in Reston, VA. Additionally, a technical training and assistance agreement exists between the CNCS Grants office and the Aguirre Hosting Corporation for the Web-based Reporting System (WBRS). The CNCS also maintains active contracts and MOUs with contractor-provided facilities for both the public web site and the DRS. Having these documented and agreed-upon policies, requirements, roles and responsibilities between the Corporation and critical "partners" in place further enhances the security and sustainment of critical operations and resources.

### Recommendations

- Based on findings associated with CNCS management of continuity of operations for IT systems, we recommend that CNCS continue to follow established procedures consistent with periodic review and update as dictated by the dynamic nature of the threat environment.

## Configuration Management

### Conclusions and Findings

**Configuration Management (CM) of CNCS systems and assets is performed in a very effective manner.** All hardware is maintained by an inventory tracking system managed by the OIT. This inventory is reviewed at least once annually as required by FISM, 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 Configuration Control Boards (CCBs), with budget decisions 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.

**CNCS has no single source document for maintaining the Corporation's inventory of major systems and their inter-connections with other systems.** FISMA guidance requires "the head of each agency to develop and maintain an inventory of major information systems (including national security systems) operated by or under the control of the agency." The Corporation identifies their major systems in a variety of methods, such as Exhibit 300s, Security Plans and the IM Strategic Plan. Although the CNCS references their systems in these various documents, the current condition has resulted in different lists reflecting inconsistencies in what systems exist and which ones are major systems. Establishing a single authoritative source listing of the Corporation's systems could rectify this problem. The official listing should also indicate the criteria used for categorizing the systems. The resulting list should then be used as the official inventory of CNCS major systems, along with their interconnections with other systems.

## Recommendations

Based on findings associated with configuration management, we recommend that CNCS review the following recommendation and take actions as necessary to enhance the agency's security program.

- Continue to conform to the proven configuration management procedures that are currently in place.

- Develop a single-source inventory of major systems.

## Consolidated List of Recommendations

A recapitulation of all corrective action recommendations contained in this report follows.

- Include test provisions in the SDLC.
- Include COTS evaluation provisions in the SDLC.
- Develop E-SPAN and e-Grants rules of behavior.
- Include system security plan summaries into the IM Strategic Plan.
- Document the procedure for conducting annual tests and evaluation in a written policy.
- Review the results of the internal and external penetration tests conducted by Carson Associates during this evaluation, and resolve/mitigate vulnerabilities, as appropriate, to meet the security needs of the Corporation and its external customers.
- Track IT security weaknesses and recommendations in single integrated process consisting of both agency-wide and system-level POA&Ms.
- Implement POA&Ms as the authoritative management tool for tracking IT security weaknesses.
- Increase CNCS functional leader and OIG involvement in the POA&M process.
- Develop a single-source inventory of major systems.

## Response to Agency Comments

At an exit conference held on August 21, 2003, CNCS officials generally agreed with the findings. The comments provided by the CNCS and OIG officials on August 26, 2003, have been incorporated in the report where appropriate.

Upon review of the draft report, CNCS officials provided a formal response to the report and recommendations contained therein. This response is provided at Appendix C.

## OBJECTIVE, SCOPE AND METHODOLOGY

The overall objective of this independent audit was to assist the OIG in meeting its FISMA obligation for independent assessment of CNCS's information security program in accordance with OMB fiscal year 2003 reporting guidelines. In support of this objective, the audit team conducted a high-level, qualitative review of the CNCS 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 CNCS. Systems examined were:

- Momentum
- E-Grants
- E-SPAN
- Corporation Network

The following describes systems and sites that were not included in the scope of this audit:

- This audit also did not include analysis of the Web-based Reporting System (WBRS). This system is a CNCS major application, but was not included by the OIG as a system to be reviewed.
- The OIG LAN was also excluded from the scope of this study.
- Additionally, this study did not include site surveys of Service Centers or contractor-operated facilities.

The scope of work was organized into three tasks:

- Background Review
- Audit Fieldwork
- Audit 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 (FISCAM) and OMB security criteria] to the following CNCS staff:

- Deputy CIO (Representing the Agency Head, CIO and Program Officials)
- Selected OIG staff members
- Selected system users

The document review process included agency:

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

An internal penetration test was conducted to evaluate security aspects of the agency's servers, printer, workstations and network infrastructure from inside the CNCS firewall. The test was performed from inside the CNCS 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 agency's firewall. The test was performed from outside the CNCS security perimeter (e.g., from the Internet). Network vulnerability scans were performed using SAINT™.

All 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
- National Institute of Standards and Technology Special Publication 800-26, *Self-Assessment Guide for Information Technology Systems*, August 2001
- OMB reporting instructions
- Information Systems Audit & Control Association standards
- CNCS OIG Audit Guidance

The evaluation was conducted on site at CNCS headquarters, 1201 New York Avenue, NW., Washington, DC 20525, between July 21 and August 27, 2003. Evaluators were Karen Frey, Randy Laudermilk, Jane Laroussi, Anthony Van Dyck and Diane Reilly from Richard S. Carson & Associates, Inc., 4720 Montgomery Lane, Suite 800, Bethesda, MD 20814.

# EXECUTIVE SUMMARY FOR MANAGEMENT AND BUDGET (OMB)

# OFFICE OF INSPECTOR GENERAL
# CORPORATION FOR NATIONAL AND COMMUNITY SERVICE

**Executive Summary for**
**Office of Management and Budget (OMB)**
**Pertaining to**
**Office of Inspector General**
**Review of Corporation for National and Community Service**
**Implementation of the Federal Information Security Management Act**
**For Fiscal Year 2003**

**OIG Audit Number 03-26**
**August 21, 2003**

Prepared by:

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

**This report was issued to Corporation management on September 18, 2003. Under the laws and regulations governing audit follow up, the Corporation must make final management decisions on the report's findings and recommendations not later than March 18, 2004, and complete its corrective actions by September 18, 2004. Consequently, the report findings do not necessarily represent the final resolution of the issues presented.**

## BACKGROUND

Richard S. Carson & Associates, Inc. (Carson Associates), on behalf of the Office of Inspector General (OIG) of the Corporation for National and Community Service (CNCS), completed an independent audit of the Corporation's implementation of the Federal Information Security Management Act (FISMA) for Fiscal Year (FY) 2003. The Independent Audit Report provides specific findings and conclusions and, when applicable, identifies problem areas and makes recommendations for resolution. This Executive Summary for the Office of Management and Budget (OMB), reports the results of this CNCS independent audit.

On December 17, 2002, President George W. Bush signed into law the E-Government Act of 2002 (Pub. L. No. 107-347), which includes Title III, the Federal Information Security Management Act of 2002 (FISMA). The FISMA permanently reauthorized the framework laid out in the Government Information Security Reform Act of 2000 (GISRA), which expired in November 2002. The FISMA outlines the information security management requirements for agencies, including the requirement for annual review and independent assessment by agency inspectors general. In addition, FISMA includes new provisions aimed at further strengthening the security of the Federal government's information and information systems, such as the development of minimum standards for agency systems. The annual assessments provide agencies with the information needed to determine the effectiveness of overall security programs, and to develop strategies and best practices for improving information security.

The independent audit comprises four elements: evaluation of CNCS's information security program, evaluation of CNCS progress towards correcting weaknesses addressed within the 2002 Plan of Action and Milestones (POA&Ms), review of the self-assessments and verification and testing of information security controls for four representative information systems. The results of the independent audit address the problems identified during the evaluation. The major findings from the report are summarized in the Results in Brief.

## PURPOSE

The objectives of the independent audit of CNCS's information security program were to:

- Test the effectiveness of information security policies, procedures and practices of a representative subset of the agency's information systems;
- Assess compliance with FISMA and related information security policies, procedures, standards and guidelines; and
- Conduct follow-up assessment of agency progress in correcting weaknesses identified in prior GISRA/FISMA evaluations, including those weaknesses listed in the Fiscal Year 2002 POA&M.

## RESULTS IN BRIEF

CNCS has taken a number of steps during the past year to enhance their security program and address issues identified in the 2002 GISRA report. These enhancements are as follows:

- Hardware and software have been acquired and installed to provide continuity of operations for the e-Grants system.

- The Continuity of Operations Plan has been successfully tested for e-Grants, with full capability anticipated by the end of this fiscal year.

- Certification and Accreditations were completed for all major applications during this reporting period.

- Improvements have been made to the test planning and execution process. Efforts are ongoing to integrate these improvements into the formal Systems Development Lifecycle methodology.

- CNCS maintains a very effective security awareness program; all employees and contractors, requiring system access, undergo annual security awareness training.

- Configuration Management policies include extensive work in the tracking of hardware inventory and software licensing, as well as the use of automation tools to track system-level configurations for desktop deployment and configuration control.

Notwithstanding the improvements stated above, some areas showed little progress toward remediation and/or did not adhere to OMB A-130 guidance. These areas were identified as problems.

- The lack of system-level rules of behavior for the Electronic-System for Program Agreements and National Service Participants (E-SPAN), and e-Grants was identified as a weakness in last year's GISRA assessment, but have not been documented or addressed to date. There are a variety of policies and procedures for the agency that are used by these system users and many cover "rules" that affect the applicable systems; however, program officials have not defined system-specific rules as required by OMB A-130.

- The 2002 GISRA report stated that a summary of major system security plans was not included in the Corporation's Information Management Strategic Plan. This item is identified in the agency-wide POA&M but, to date, has not been included in the Information Management Strategic Plan. However, during an August 2003 interview with the Corporation's Deputy Chief Information Officer, (currently the position of Chief Information Officer is vacant), it was found that this weakness is now being addressed and should be resolved upon publication of the revised plan this year.

- The Corporation has a stated policy to perform complete Certification and Accreditation processes each year (versus every 3 years or whenever a major system change occurs) for all major systems, rather than performing annual tests and evaluations as defined in OMB A-130. However, there is no documented policy within CNCS stating annual System Test and Evaluation and risk assessment processes will be accomplished as a part of Certification and Accreditation.

- The Corporation's corrective action process needs to be improved to ensure that all Information Technology (IT) security weaknesses are identified on system-level POA&Ms and that the program officials and Inspector General track and support resolution of these actions in a pro-active, collaborative way. The Corporation's Deputy Chief Information Officer and Office of Inspector General maintain a variety of tracking systems and maintain their own processes. However, the POA&M process, as described

by OMB A-130 and recent FISMA reporting Guidance (August 6, 2003), is not the Corporation's authoritative management tool for tracking IT security weaknesses.

- The Corporation identifies their major systems in a variety of methods, such as Exhibit 300s, Security Plans and the Information Management Strategic Plan. However, there is no single source for maintaining the Corporation's inventory of major systems and their inter-connections with other systems. The resulting condition is a lack of reconciliation between documents and reporting methods concerning the official list of major systems within CNCS.

## RECOMMENDATIONS

The Independent Audit Report includes 10 recommendations to strengthen the CNCS security program.

## A. OVERVIEW OF FISMA IT SECURITY REVIEWS

**A.2a. Identify the total number of programs and systems in the agency, the total number of systems and programs reviewed by the program officials and CIOs in FY03, the total number of contractor operations or facilities, and the number of contractor operations or facilities reviewed in FY03. Additionally, IGs shall also identify the total number of programs, systems, and contractor operations or facilities that they evaluated in FY03.**

| Bureau Name | FY03 Programs | | FY03 Systems | | FY03 Contractor Operations or Facilities | |
|---|---|---|---|---|---|---|
| | Total Number | Number Reviewed | Total Number | Number Reviewed | Total Number | Number Reviewed |
| CNCS | 3 | 3 | 5 | 3 | 2 | 2 |
| | | | | | | |
| **Agency Total** | 3 | 3 | 5 | 3 | 2 | 2 |
| **b. For operations and assets under their control, have agency program officials and the agency CIO used appropriate methods (e.g., audits or inspections, agreed upon IT security requirements for contractor provided services or services provided by other agencies) 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?** | Yes | | | Yes | | |
| **c. If yes, what methods are used? If no, please explain why.** | CNCS used several methods. CNCS has recently reviewed the Statement on Auditing Standards (SAS) 70 report on the Department of Interior's National Business Center in Reston, VA. CNCS also maintains SAS 70 reports on the Department of Health and Human Services and the National Finance Center systems to address interconnections between their respective systems. Additionally, a technical training and assistance agreement exists between the CNCS Grants office and the Aguirre Hosting Corporation for the Web-based Reporting System (WBRS), as well as contracts with various contractors to ensure compliance with security requirements. The effect on CNCS of having these mechanisms in place is a documented set of policies, requirements, roles and responsibilities between the Corporation and critical "partners" to further enhance the security and sustainment of critical operations and resources.<br><br>CNCS also used the self-assessment guide as outlined in NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems, in 2002 and 2003 during the development of Security Plans.<br><br>During 2003, CNCS followed OMB A-130 guidelines, by using NIST's Security Self-Assessment Guide for Information Technology Systems (SP 800-26) in their security plan review of the Momentum System, maintained by the National Business Center. Additionally, CNCS NIST's Risk Management Guide for Information Technology Systems, (SP 800-30) in the performance of a risk assessment for Momentum, during the re-certification and accreditation of Momentum. | | | | |
| **d. Did the agency use the NIST self-assessment guide to conduct its reviews?** | Yes | | Yes | | | |
| **e. If the agency did not use the NIST self-assessment guide and instead used an agency-developed methodology, please confirm that all elements of the NIST guide were addressed in the agency methodology.** | Yes | | Yes | | | |

| | |
|---|---|
| **f. Provide a brief update on the agency's work to develop an inventory of major IT systems.** | The Corporation describes its systems within its Information Management Strategic Plan to document all systems, to include major applications, general support systems, and "other" systems not deemed vital to CNCS operations. CNCS also maintains Exhibit 300s and C&As for systems deemed major applications to the critical operations of CNCS. The Deputy Chief Information Officer has deemed this method of "inventory" appropriate since the number of major applications is small. |

CNCS programs include Senior Corps, AmeriCorps and Learn and Serve America. CNCS currently uses, operates or owns three major applications and one general support system. The Office of Inspector General operates its own general support system. The systems list follows.

Major Applications:

- Momentum [operated by the Department of Interior's National Business Center].
- Electronic-System for Program Agreements and National Service Participants which also includes the e-Grants module.
- Web-based Reporting System, (WBRS), maintained by the Aguirre Hosting Corporation.

General Support Systems:

- CNCS Network.
- CNCS OIG Local Area Network.

**A.3. Identify all material weakness in policies, procedures, or practices as identified and required to be reported under existing law in FY03. Identify the number of material weaknesses repeated from FY02, describe each material weakness, and indicate whether POA&Ms have been developed for all of the material weaknesses.**

| | FY03 Material Weaknesses | | | |
|---|---|---|---|---|
| **Bureau Name** | Total Number | Total Number Repeated from FY02 | Identify and Describe Each Material Weakness | POA&Ms developed? Y/N |
| CNCS | 0 | 0 | | |
| | | | | |
| **Agency Total** | 0 | 0 | | |

No material weaknesses were identified for CNCS during the course of this assessment.

| **A.4. This question is for IGs only. Please assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestone process that meets the criteria below. Where appropriate, please include additional explanation in the column next to each criterion.** | **Yes** | **No** |
|---|---|---|
| Agency program officials develop, implement, and manage POA&Ms for every system that they own and operate (systems that support their programs) that has an IT security weakness. | | No (see note) |
| Agency program officials report to the CIO on a regular basis (at least quarterly) on their remediation progress. | Yes (see note) | |
| Agency CIO develops, implements, and manages POA&Ms for every system that they own and operate (systems that support their programs) that has an IT security weakness. | Yes (see note) | |
| The agency CIO centrally tracks and maintains all POA&M activities on at least a quarterly basis. | Yes (see note) | |
| The POA&M is the authoritative agency and IG management tool to identify and monitor agency actions for correcting information and IT security weaknesses. | | No (see note) |

| | | |
|---|---|---|
| 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) to tie the justification for IT security funds to the budget process. | | No (see note) |
| Agency IGs are an integral part of the POA&M process and have access to agency POA&Ms. | Yes (see note) | |
| The agency's POA&M process represents a prioritization of agency IT security weaknesses that ensures that significant IT security weaknesses are addressed in a timely manner and receive, where necessary, appropriate resources. | | No (see note) |

There is a single agency POA&M that is managed by the Deputy Chief Information Officer, acting as the Program Official for all systems. There are other mechanisms throughout CNCS that track various types of action items related to agency systems.

The Deputy Chief Information Officer acts as the Program Official for all CNCS systems. He is an integral part of all phases of the lifecycle process, including remediation of POA&M items.

A single POA&M is developed and managed by the Deputy Chief Information Officer that includes an aggregate of IT security weaknesses for all major applications.

The Deputy Chief Information Officer maintains the agency-wide POA&M and reports the status on a quarterly basis. Other tracking mechanisms are currently in place to track action items.

Currently, there is a single agency-wide POA&M. There are no "system-level" POA&Ms identified by the Corporation's Exhibit 300 identification to tie to business cases.

The agency Office of Inspector General is involved in the POA&M process in two critical areas. First, it reviews POA&M items during financial audits to ensure compliance with financial regulations. Second, it provides an oversight role to ensure that FISMA independent assessments are conducted on a yearly basis. Additionally, the Office of Inspector General is involved during system design and re-design phases to offer input into "auditable issues" to the functional and technical members of the design team.

The agency-wide POA&M contains a list of significant IT security weaknesses and represents a prioritization of those items. However, there are no system-level POA&Ms maintained at this time to ensure tracking of system-specific IT security weaknesses.

## B. RESPONSIBILITIES OF AGENCY HEAD

For the purposes of this report, the CNCS agency head is the Chief Financial Officer.

| | |
|---|---|
| **B.1. Identify and describe any specific steps taken by the agency head to clearly and unambiguously set forth FISMA's responsibilities and authorities for the agency CIO and program officials. Specifically how are such steps implemented and enforced?** | The Chief Operating Officer (COO) approves agency-wide policies related to the use and operation of IT resources. The Deputy CIO executes these policies and acts as the Program Official for all systems within CNCS. Additionally, the Chief Financial Officer (CFO) is the approval authority for budget requests submitted through the CNCS Change Control Board (CCB). |
| **B.2. Can a major operating component of the agency make an IT investment decision without review by and concurrence of the agency CIO?** | No CNCS operating component can make an IT investment decision without coordinating the requirement through the CCB and coordinating through the Deputy CIO (CIO position currently vacant). The Deputy CIO is directly involved in the process and is involved in any budget approvals made by the CFO from IT budget requests. |

| | |
|---|---|
| **B.3. How does the head of the agency ensure that the agency's information security plan is practiced throughout the life cycle of each agency system?** | The Deputy CIO is directly involved in the development and execution of a Systems Development Lifecycle methodology. The Deputy CIO is also directly involved in the development of system-level Security Plans, the CNCS Business Continuity/Contingency Plan (BCCP) and system Continuity of Operations Plan (COOP). |
| **B.4. During the reporting period, did the agency head take any specific and direct actions to oversee the performance of 1) agency program officials and 2) the CIO to verify that such officials are ensuring that security plans are up-to-date and practiced throughout the lifecycle of each system?** | The Deputy CIO acts as the program official for all major and general support systems and ensures security plans are uptodate and practiced throughout the lifecycle of each system. |
| **B.5. Has the agency integrated its information and information technology security program with its critical infrastructure protection responsibilities, and other security programs (e.g., continuity of operations, and physical and operational security)? Please describe.** | Decisions concerning information system impact on CNCS's critical infrastructure is made collaboratively between the Deputy CIO and functional area leaders of the three critical programs. Security and continuity of operation is maintained to the level deemed appropriate by agency officials. BCCP and COOP plans are updated and tested periodically to ensure critical systems can be recovered in the event of failure. The Deputy CIO's staff maintains current procedures for coordinating with FedCIRC and other security agencies in the event of an attack. |
| **B.6. Does the agency have separate staffs devoted to other security programs, are such programs under the authority of different agency officials, if so what specific efforts have been taken by the agency head or other officials to eliminate unnecessary duplication of overhead costs and ensure that policies and procedures are consistent and complimentary across the various programs and disciplines?** | CNCS security programs are decentralized according to the type of security program. The Office of Information Technology develops and maintains security programs for both telecommunications and information security for resources under their control. Physical security for access to CNCS office space is managed by CNCS Administrative Services through the use of badges and Kastle keys. Physical security for the New York Avenue headquarters facility is maintained by building management. Functional area leaders are responsible for controlling physical access to their facilities and systems resources, as well as for information and document security by users under their area of responsibility. Duplication of responsibilities and overhead cost are eliminated by defining the boundaries of the various security programs and management involvement when determining by whom and where these programs will be maintained. |

| **B.7. Identification of agency's critical operations and assets (both national critical operations and assets and mission critical) and the interdependencies and interrelationships of those operations and assets.** | | | | |
|---|---|---|---|---|
| **a. Has the agency fully identified its national critical operations and assets?** | Yes | ✓ | No | |
| **b. Has the agency fully identified the interdependencies and interrelationships of those nationally critical operations and assets?** | Yes | ✓ | No | |
| **c. Has the agency fully identified its mission critical operations and assets?** | Yes | ✓ | No | |
| **d. Has the agency fully identified the interdependencies and interrelationships of those mission critical operations and assets?** | Yes | ✓ | No | |

| | |
|---|---|
| e. If yes, describe the steps the agency has taken as a result of the review. | The agency maintains the detailed description of agency systems, their support to critical operations and interdependencies in the IM Strategic Plan. This plan is being updated during 2003 to describe the methodology for identifying major applications and for enhancing the description of interdependencies and interrelationships. |
| f. If no, please explain why. | N/A |

| B.8. How does the agency head ensure that the agency, including all components, has documented procedures for reporting security incidents and sharing information regarding common vulnerabilities? | | | | |
|---|---|---|---|---|
| a. Identify and describe the procedures for external reporting to law enforcement authorities and to the Federal Computer Incident Response Center (FedCIRC). | CNCS OIT developed the Computer Incident Response Guidelines to provide OIT and end users with the procedures for reporting incidents. This document was updated in July 2002. All users will notify the Deputy CIO and/or the ISSO immediately when an incident occurs. The Deputy CIO or Information Systems Security Officer then determines the next course of action, whether that includes notifying law enforcement and/or FedCIRC. The Deputy CIO and ISSO are directly involved in the process to ensure all procedures are followed according to CNCS and FedCIRC policy. Physical security incidents are reported to CNCS Administrative Services, which in turn, notifies the Washington D.C. Police Department (WPD) or Federal Protective Service as required. | | | |
| b. Total number of agency components or bureaus. | 1 | | | |
| c. Number of agency components with incident handling and response capability. | 1 - All agency incident handling and response capability is supported through CNCS OIT. | | | |
| d. Number of agency components that report to FedCIRC. | 1 | | | |
| e. Does the agency and its major components share incident information with FedCIRC in a timely manner consistent with FedCIRC and OMB guidance? | Yes | | | |
| f. What is the required average time to report to the agency and FedCIRC following an incident? | 3 Hours | | | |
| g. How does the agency, including the programs within major components, confirm that patches have been tested and installed in a timely manner? | CNCS OIT develops and implements all patch policies within the agency. Internal intrusion detection software is run to detect patch level. When a patch is required, it is first installed on a test platform and verified. The patch is then applied to the production platform and verified. The intrusion detection scan is run again to validate the patch and ensure no other patches are required. | | | |
| h. Is the agency a member of the Patch Authentication and Distribution Capability operated by FedCIRC? | Yes | ✓ | No | |
| i. If yes, how many active users does the agency have for this service? | 3 | | | |
| j. Has the agency developed and complied with specific configuration requirements that meet their own needs? | Yes | ✓ | No | |
| k. Do these configuration requirements address patching of security vulnerabilities? | Yes | ✓ | No | |

| B.9. Identify by bureau, the number of incidents (e.g., successful and unsuccessful network penetrations, root or user account compromises, denial of service attacks, website defacing attacks, malicious code and virus, probes and scans, password access) reported and those reported to FedCIRC or law enforcement. | | | |
|---|---|---|---|
| Bureau Name | Number of incidents reported | Number of incidents reported externally to FedCIRC | Number of incidents reported externally to law enforcement |
| CNCS | 0 | 0 | 0 |

There have been no successful incidents during this fiscal year. This result is as of August 27, 2003.

## C. RESPONSIBILITIES OF AGENCY PROGRAM OFFICIALS AND AGENCY CHIEF INFORMATION OFFICERS

For the purposes of this report, the CNCS program official is the Deputy Chief Information Officer.

| C.1. Have agency program officials and the agency CIO: 1) assessed the risk to operations and assets under their control; 2) determined the level of security appropriate to protect such operations and assets; 3) maintained an up-to-date security plan (that is practiced throughout the life cycle) for each system supporting the operations and assets under their control; and 4) tested and evaluated security controls and techniques? By each major agency component and aggregated into an agency total, identify actual performance in FY03 according to the measures and in the format provided below for the number and percentage of total systems. | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Bureau Name | Total Number of Systems | Number of systems assessed for risk and assigned a level or risk | | Number of systems that have an up-to-date IT security plan | | Number of systems certified and accredited | | Number of systems with security control costs integrated into the life cycle of the system | | Number of systems for which security controls have been tested and evaluated in the last year | | Number of systems with a contingency plan | | Number of systems for which contingency plans have been tested | |
| | | No. of Systems | % of Systems | No. | % | No. | % | No. | % | No. | % | No. | % | No. | % |
| CNCS | 3 | 3 | 100% | 3 | 100% | 3 | 100% | 3 | 100% | 3 | 100% | 3 | 100% | 3 | 100% |
| | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | |
| Agency Total | 3 | 3 | 100% | 3 | 100% | 3 | 100% | 3 | 100% | 3 | 100% | 3 | 100% | 3 | 100% |

During 2002-2003, a complete Certification and Accreditation process was executed for the e-Grants module of E-SPAN, resulting in a total of four for each of the categories defined above. However, now that e-Grants is classified as a module of the E-SPAN major system, the numbers provided above include e-Grants as part of E-SPAN.

| C.2. Identify whether the agency CIO has adequately maintained an agency-wide IT security program and ensured the effective implementation of the program and evaluated the performance of major agency components. | | | | |
|---|---|---|---|---|
| Has the agency CIO maintained an agency-wide IT security program? Y/N | Did the CIO evaluate the performance of all agency bureaus/components? Y/N | How does the agency CIO ensure that bureaus comply with the agency-wide IT security program? | Has the agency CIO appointed a senior agency information security officer per the requirements in FISMA? | Do agency POA&Ms account for all known agency security weaknesses including all components? |
| Yes | Yes | The Deputy CIO acts on behalf of the CIO (position currently vacant) and fulfills the role of program | Yes | No. Currently there are a number of tracking mechanisms used by CNCS, based on the type |

| | | | | |
|---|---|---|---|---|
| | | official for all major and general support systems. There are no separate bureaus within CNCS. Programs support specific CNCS business areas. All security-related issues from program functional area leaders are coordinated through the Deputy CIO, OIT and the Information System Security Office. | | of issue and area of responsibility in responding to them. It has been recommended by the FISMA assessment team that CNCS evaluate the current process and tracking mechanisms to develop a process that ensures that agency-wide and system-level POA&Ms account for all known security weaknesses. |

| C.3. Has the agency CIO ensured security training and awareness of all agency employees, including contractors and those employees with significant IT security responsibilities? | | | | | | | |
|---|---|---|---|---|---|---|---|
| Total number of agency employees in FY03 | Agency employees that received IT security training in FY03 | | Total number of agency employees with significant IT security responsibilities | Agency employees with significant security responsibilities that received specialized training | | Briefly describe training provided | Total costs for providing training in FY03 |
| | Number | Percentage | | Number | Percentage | | |
| 606 | 659 | 109% | 7 | 7 | 100% | In additional to the annual security awareness training, these individuals receive training through FedSec and on-line training sites (such as the VPN security class through on-line webcase), as well as utilizing various security organization websites, trade shows and publications to remain aware of current security issues. | $27K |

All employees and contractors that require access to systems or sensitive data must undergo IT security awareness training before obtaining accounts and access to the applicable data. The number of agency employees, as of July 30, 2003, is 606. The number of employees that received training during FY 2003 includes current employees and those who received training during this fiscal year, but left the Corporation prior to July 30, 2003. The next formal "annual" training is scheduled for December 2003 (FY 2004).

| C.4. Has the agency CIO fully integrated security into the agency's capital planning and investment control process? Were IT security requirements and costs reported on every FY05 business case (as well as in the exhibit 53) submitted by the agency to OMB? | | | | |
|---|---|---|---|---|
| Bureau Name | Number of business cases submitted to OMB in FY05 | Did the agency program official plan and budget for IT security and integrate security into all of their business cases? Y/N | Did the agency CIO plan and budget for IT security and integrate security into all of their business cases? Y/N | Are IT security costs reported in the agency's exhibit 53 for each IT investment? Y/N |
| CNCS | 3 | Yes | Yes | Yes |

CNCS has not completed business cases for FY 2005; therefore, values for the questions in C.4. above were not available at the time of this report. The current plan is to develop three business cases based on the Momentum, WBRS and E-SPAN major applications. A fourth business case may be included for the infrastructure, based on a resolution of current OMB guidance on steady-state systems and architectures previously not considered major applications.

As of the date of this report, specific requirements were not defined within the FY 2005 business cases. Historically, CNCS program officials plan and budget IT security requirements as they apply to each business case. However, reporting may be "rolled" into a specific business case due to the consolidated infrastructure that affects the security implementation across one or multiple systems. The method for defining security requirements is dependent upon defined security requirement(s) and/or planned execution of the budget to support them. At this time, there is no specific material to state factually that individual FY 2005 business cases will not contain security information. Thus, the current plan is to state them by business case.

# AGENCY RESPONSE TO OIG FY 2003 FISMA REPORT

Corporation for
NATIONAL & COMMUNITY SERVICE

September 10, 2003

The Honorable Russell George,
Inspector General
Corporation for National and Community Service

Dear Mr. George:

The Corporation has reviewed the draft report *Review of the Corporation for National and Community Service Implementation of the Federal Information Security Management Act* (OIG Audit Report 03-26, dated August 21, 2003). The purpose of Richard S. Carson & Associates' (Carson & Associates) work was to review the Corporation's information systems security program and assess the effectiveness of the program. The procedures performed by Carson & Associates included sophisticated attempts to penetrate the Corporation's systems as both an "outside" hacker and an "insider." We note with satisfaction that Carson & Associates found two minor security vulnerabilities that were only discovered once they were given access to the network and that they were unsuccessful in their external attempts to penetrate the Corporation's systems.

The Corporation is also pleased that, Carson & Associates concluded that the Corporation's systems security program is effective and efficient. The Corporation has taken the security of its computer resources very seriously and will continue to do so. To this end, the Corporation routinely tests and monitors its systems and contracts with independent EDP consultants to review and test its systems. We also rely on the testing and review that was performed by Carson & Associates on behalf of the Office of the Inspector General and discussed in this report.

The report cites a single theme which Carson & Associates feels that the Corporation should focus upon - documentation. There are five specific recommendations for improved documentation. The first of these recommendations is for the development of a set of system-level rules of behavior for eSPAN. While we believe that the rules of behavior for eSPAN are set and followed through a series of processes, including the configuration of the system, the Corporation will develop a formal document to address this recommendation.

In the second recommendation, Carson & Associates reiterated an earlier finding that has been reported on our quarterly Plans of Action and Milestone (POA&M) reports to OMB; but has yet to be completed. This recommendation is to include in the Corporation's Strategic Plan a summary of its major systems security plans. The Corporation's Strategic Plan is currently being revised and will include these summaries.

The final three recommendations center on the process involved in performing reviews of the Corporation's security program. These recommendations call for the development of three documents that would assist in defining the Corporation's approach

to security reviews. The Corporation agrees with these recommendations and will develop documents that will define our yearly accreditation process; specifically document how the Corporation classifies systems and what its major systems are; and develop an overall POA&M process which will provide single point for tracking future IT audit recommendations.

* * * * * * * * * * * * * * * * * * * * * *

Finally, the Corporation would like to express its appreciation for the work of Carson & Associates staff and their flexibility to work around the other pressing responsibilities of the Corporation staff.

Sincerely,

Michelle Guillermin
Chief Financial Officer