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

# OIG Audit Report Regarding Corporation for National and Community Service Evaluation of Information Systems Pursuant to the Government Information Security Reform Act

**OIG Audit Report Number 02-35**
**September 16, 2002**

Prepared by:

KPMG, LLP
2001 M Street, NW
Washington, DC 20036

Under Corporation for National and Community Service OIG Contract
With the General Services Administration
GSA Contract No. GS-23F-8127H
Order Number CNSIG-02-G-0007

---

**This report was issued to Corporation management on September 16, 2002. Under the laws and regulations governing audit follow up, the Corporation must make final management decisions on the report's findings and recommendations no later than March 16, 2003, and complete its corrective actions by September 16, 2003. Consequently, the reported findings do not necessarily represent the final resolution of the issues presented.**

---

Office of Inspector General
Corporation for National and Community Service
Performance Audit of Information Systems Pursuant to
the Government Information Security Reform Act (GISRA)

Table of Contents

KPMG LETTER REPORT

RESULTS IN BRIEF ..... 1

PROJECT OBJECTIVES ..... 2

METHODOLOGY ..... 2

FY 2002 GISRA REPORT

EXECUTIVE SUMMARY - RESPONSES TO OMB QUESTIONS ..... 1

GENERAL OVERVIEW ..... 2

RESPONSIBILITIES OF AGENCY HEAD ..... 3

RESPONSIBILITIES OF AGENCY PROGRAM OFFICIALS ..... 7

RESPONSIBILITIES OF AGENCY CHIEF INFORMATION OFFICER ..... 8

APPENDIX A - CHART 1 - GISRA OVERALL ASSESSMENT SUMMARY ..... A-1

APPENDIX B - GISRA ASSESSMENT SUMMARY OF AGENCY-WIDE POLICIES AND PROCEDURES ..... B-1

APPENDIX C - GISRA ASSESSMENT SUMMARY OF LOCAL AND WIDE AREA NETWORKS ..... C-1

APPENDIX D - GISRA ASSESSMENT SUMMARY OF MOMENTUM ..... D-1

APPENDIX E - GISRA ASSESSMENT SUMMARY OF SYSTEM FOR PROGRAMS, AGREEMENTS AND NATIONAL PARTICIPANTS ..... E-1

September 16, 2002

Russell George
Inspector General
Corporation for National and Community Service
Washington, DC 20525

Dear Mr. George:

At your request, KPMG LLP (KPMG) conducted a performance audit of the Corporation for National and Community Service's compliance with the Government Information Security Reform Act (GISRA) and the implementing guidance issued by the Office of Management and Budget (OMB) in OMB Memorandum M-02-09. GISRA focuses on the management of each agency's information security program, and directs that information security vulnerabilities and their remediation be explicitly considered when the agency annually considers its budget needs, priorities and allocation of funding. As required by OMB, our evaluation used Special Publication 800-26, Information Security Self-Assessment Guide, issued by the Department of Commerce, National Institute of Standards and Technology (NIST), in conjunction with the corollary CIO Council's Federal Information Technology Security Assessment Framework. The objectives of our evaluation were 1) to assess compliance of the Corporation's management of its information security program, 2) to assess compliance of the Corporation's operational and technical implementation of its information security program, and 3) to test the effectiveness of the Corporation's operational and technical implementation of its information security program.

## *Results in Brief*

The GISRA assessment this year showed that the Corporation has made a few modest improvements in its security policies and procedures documentation, but has continued to place its primary emphasis on the operational aspects of maintaining information security and on implementing e-Grants, a major new application system. OMB's GISRA guidance directs agencies to adopt the NIST Security Self-Assessment, or an equivalent tool that heavily emphasizes the need to document an agency's security policies, procedures and practices, and to document that agency personnel review and verify their implementation. Achieving the level of documented procedures and verification envisioned by GISRA and the NIST Security Self-Assessment poses a substantial challenge for a small agency like the Corporation. During the past year, these documentation requirements did not receive as much of the Corporation's attention as its operational security concerns. However, the lack of incidents and the results of external penetration testing demonstrate that the Corporation's critical systems were effectively protected.

An underlying condition that affects the Corporation's ability to comply with all GISRA requirements is the consistent lack of Information Technology (IT) resources. The Corporation's small IT staff places priority on operational matters and keeping pace with technological change. It often has little or no residual capacity for improving documentation and procedures. That has been especially true in FY 2002, when the Corporation developed a new application system to support one of its most significant missions, grants management.

Current Corporation security policies generally instruct that there be compliance with GISRA, however, the accompanying procedures have not been updated to reflect the expanded responsibilities of program officials and the need for routine, annual security assessments using the NIST self-assessment methodology. In early FY 2001 as part of the re-accreditation of its systems, the Corporation had a contractor perform a risk analysis, vulnerability assessment and an update to the system security plan for each of its systems. That work substantially met the intent of the GISRA requirement for assessments. In mid-August 2002 a contractor was engaged to conduct a GISRA assessment based on the NIST methodology.

The lack of any security incidents or breaches in FY 2002 indicates that at an operational level the Corporation has maintained effective security for its systems. However, it does not have security consistently integrated into its planning, budgeting, documented procedures and routine testing as envisioned by GISRA legislation and regulation.

## *Project Objectives*

Our objectives were to conduct an independent evaluation of the Corporation's information security program and practices, to test the effectiveness of the Corporation's security control techniques, and to ascertain the Corporation's degree of compliance with the Government Information Security Reform Act (GISRA) and implementing guidance from OMB.

## *Methodology*

OMB Memorandum 02-09 requires the use of the NIST "Security Self-Assessment Guide for Information Technology Systems", NIST Special Publication 800-26 (The NIST Guide) and the corollary CIO Council's "Federal Information Technology Security Assessment Framework" (The Framework). Together they provide a vehicle for a consistent and effective measurement of the security status for a given asset.

The NIST Guide provides specific questions that identify the control criteria against which agency policies, procedures and security controls are evaluated.

The Framework is divided into five levels: Level 1 of the Framework reflects that an asset has documented security policies. At Level 2, the asset also has documented procedures and controls to implement the policies. Level 3 indicates that procedures and controls have been implemented. Level 4 shows that the procedures and controls are tested and reviewed. At Level 5, the asset has procedures and controls that are fully integrated into a comprehensive

life cycle program and into the strategic planning and resource allocation processes of the agency. The evaluation of the Corporation's assets was performed in accordance with the NIST Guide methodology in the same four areas that were done in FY01:

- Momentum (the Corporation's financial management system)
- SPAN (System for Programs, Agreements and National Service Participants)
- The Corporation's Network
- Agency-wide policies and procedures that are not specific to an individual system

The Web Based Reporting System (WBRS) that is due to be replaced in FY03 and the e-Grants system that is just becoming operational were not included in the evaluation.

In addition to the review of policies, procedures and practices, a Vulnerability and Penetration Assessment was performed on the Corporation's external and internal networks. The external testing showed no weaknesses in perimeter security defenses; however, internal testing of the network and servers uncovered a few procedural lapses that were easily remedied, but potentially serious if discovered by the wrong parties.

The results of the KPMG evaluations that were done using the NIST Guide's methodology are summarized in Appendices A through E, following the Executive Summary that contains responses to OMB's questions. (Detailed information to support each rating for each criteria is contained in the workpapers.) In Appendix A, Chart 1 shows the overall results for all four evaluations.

We conducted our audit in accordance with auditing standards generally accepted in the United States of America and the standards applicable to performance audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States.

*****

This report is intended solely for the information and use of the Office of the Inspector General, the management of the Corporation for National and Community Service, the Office of Management and Budget, and the United States Congress and is not intended to be and should not be used by anyone other than these specified parties.

Felipe Alonso
Partner, KPMG LLP

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

# FY 2002 GISRA Report
# Responses to OMB Questions
# Executive Summary

## Summary

The GISRA assessment this year showed that the Corporation has made a few modest improvements in its security policies and procedures documentation, but has continued to place its primary emphasis on the operational aspects of maintaining information security and on implementing e-Grants, a major new application system. OMB's GISRA guidance directs agencies to adopt the NIST Security Self-Assessment, or an equivalent tool that heavily emphasizes the need to document an agency's security policies, procedures and practices, and to document that agency personnel review and verify their implementation. Achieving the level of documented procedures and verification envisioned by GISRA and the NIST Security Self-Assessment poses a substantial challenge for a small agency like the Corporation. During the past year, these documentation requirements did not receive as much of the Corporation's attention as its operational security concerns. However, the lack of incidents and the results of external penetration testing demonstrate that the Corporation's critical systems were effectively protected.

An underlying cause for this is probably the consistent lack of Information Technology (IT) resources. The Corporation's small IT staff places priority on operational matters and keeping pace with technological change. It often has little or no residual capacity for improving documentation and procedures. That has been especially true in FY 2002, when the Corporation developed a new application system to support one of its most significant missions, grants management.

Although IT systems are relied upon for all of its major missions, CNS employees with IT responsibilities comprise only about 1.5 % of the total number of employees (9 out of more than 600). Contractor staff also support IT functions, but all together the IT staff is less than 3% of the total. While it is not the only factor, the limited number of IT resources greatly hinders the Corporation's ability to comply with all GISRA requirements.

Current Corporation security policies generally instruct that there be compliance with GISRA, however, the accompanying procedures have not been updated to reflect the expanded responsibilities of program officials and the need for routine, annual security assessments using the NIST self-assessment methodology. In early FY 2001, as part of the re-accreditation of its systems, the Corporation had a contractor perform a risk analysis, vulnerability assessment and an update to the system security plan for each of its systems. That work substantially met the intent of the GISRA requirement for assessments. In mid-August 2002 a contractor was engaged to conduct a GISRA assessment using the NIST methodology.

The lack of any security incidents or breaches in FY 2002 indicates that at an operational level the Corporation has maintained effective security for its systems. However, it does not have security consistently integrated into planning, budgeting, documented procedures and routine testing as envisioned by GISRA legislation and regulation.

The vulnerability analysis and penetration testing that were performed on the Corporation's external and internal networks showed no weaknesses in perimeter security defenses. However, internal testing of network components and servers uncovered a few procedural lapses in the installation of commercial-off-the-shelf software that were easily remedied, but potentially serious if discovered by the wrong parties. Once vulnerabilities were identified, the Corporation acted promptly, as they usually do, to fix the problems.

During the past year the Corporation has updated the documentation of its Incident Handling procedures, Systems Development Life Cycle (SDLC) procedures and the user documentation for the Momentum and SPAN systems. It has also made the Corporation's Network and Systems Security Plan an attachment to the Corporation's Strategic Plan. However, the Corporation continues to have weaknesses in the documentation of security procedures and practices, and in documentation that there is consistent verification and review of security controls and audit logs.

During FY 2002 the Corporation also made some difficult to implement changes to its Web Based Reporting System (WBRS) to improve the strength of passwords and related procedures.

The Corporation has no policies or procedures for the review of outsourced IT functions, activities, or interconnections. It relies entirely on the security provided by the other government agency or contractor.

There are no documented procedures for conducting risk assessments. The risk assessments done in conjunction with system re-accreditations in FY 2001 contain no assessment of business impact. Additionally, the Continuity of Operations (COOP) Plan has not been updated or tested since Y2K.

## A. General Overview

### 1. Total Security Funding

Per OMB guidance this information is to be provided by the Corporation.

### 2. Total Number of Programs and Systems in the Agency and Number Reviewed

In FY01:

- The IG used the complete NIST Security Self-Assessment methodology.
- The Corporation re-accredited its systems in accordance with OMB Circular A-130. The re-accreditation process covered some, but not all, of the security topics contained in the NIST Security Self-Assessment Guide.

In FY 02:

- The IG used the complete NIST Security Self-Assessment methodology.
- The CIO used the NIST Security Self-Assessment methodology.

| | FY01 | | FY02 | |
|---|---|---|---|---|
| a. Total number of agency programs. | 3 | | 3 | |
| b. Total number of agency systems. | 4 | | 5 | |
| | CIO | IG | CIO | IG |
| c. Total number of programs reviewed. | 3 | 3 | 3 | 3 |
| d. Total number of systems reviewed. | 4 | 3 | 4 | 3 |

Programs: AmeriCorps, SeniorCorps, Learn and Serve

Systems: Momentum, SPAN, WBRS, e-Grants*, LAN

* e-Grants, the Corporation's new grants management system, is included in the OIG's GISRA assessment for 2002 as a system, although it achieved only limited operational status in June 2002 and will be tested with a very limited number of grant applications prior to September 30, 2002. The Corporation's GISRA assessment does not count e-Grants as an operational system, because e-Grants will not become fully operational until FY 2003. The Corporation will fully assess and accredit e-Grants system during FY 2003.

### 3. Material Weakness in Policies, Procedures, or Practices

| | FY01 | FY02 |
|---|---|---|
| a. Number of material weaknesses reported. | 0 | 0 |
| b. Number of material weaknesses repeated in FY02. | 0 | 0 |

## B. Responsibilities of Agency Head

### 1. Specific Steps by the Agency Head to set forth the Security Act's responsibilities for the CIO and Program Officials

The paragraph below is an excerpt from the Corporation's Network and Computer Security Policy #376, effective July 2001. It is the only documented policy guidance to the CIO and Program Officials concerning their responsibilities for carrying out the Government Information Security Reform Act (GISRA).

> "The Government Information Security Reform Act requires Federal agencies to ensure that: each major system has a security plan; each responsible program official reviews that plan annually; and an independent evaluation of that review is conducted annually. The Corporation will use the accreditation work described below as the basis of this review process every

three years. In the intervening two years, each responsible program official, with the assistance of the staff of the Chief Information Officer, will prepare a brief review of changes made to the system since the past accreditation/re-accreditation. They then will certify whether the security controls described in the accreditation/re-accreditation are still adequate. The Chief Information Officer will arrange for the independent review of those certifications."

**How such steps are implemented and enforced**

Corporation management states that security responsibilities and actions of the CIO and Corporation program officials are included as part of their individual performance evaluations and were reviewed in this fiscal year.

**IT Investment Decisions**

Major operating components of the Corporation cannot make an IT investment decision without the Corporation CIO's concurrence.

2. **How the head of the agency ensures that the agency's information security plan is practiced throughout the life cycle of each agency system:**

The Corporation relies on an independent contractor to periodically conduct risk assessments, to update system security plans and to evaluate security controls. Upon receipt of the contractor's reports, the Corporation re-accredits its systems. Such accreditation first occurred in 1997, and was re-performed in August 2001. In FY 2002, the Corporation's systems were not re-accredited; however, the Corporation has a contract to have that done before December 31, 2002.

During the course of FY2002 the Corporation developed and put into limited production, a new system that for the first time automates its grants management processes, a major part of the Corporation's mission. Corporation management has contracted to have the initial risk assessment, vulnerability analysis and security plan performed later this year.

**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 that security plans are practiced throughout the lifecycle of each system**

Modifications to three of the Corporation's systems were made during the course of implementing the new grants management system. The Corporation has a contract to re-perform risk assessments, vulnerability analyses and updates to the system security plans for these three systems before December 31, 2002.

3. **How the agency has 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).**

   The Corporation has a small information technology staff that is responsible for all information security, disaster recovery and continuity of operations matters. There are no separate staff nor different officials responsible for any type of security program.

4. **Has the agency undergone a Project Matrix review?**

   The Corporation has not done a Project Matrix Review. However, The Corporation has a single communications network, and considers all of its systems to be critical, except those that are small desktop systems. All of the Corporation's systems are within one network security perimeter, with only a very limited number of external connections.

5. **How the agency head ensures that the agency has documented procedures for reporting security incidents and sharing information regarding common vulnerabilities**

   The Computer Incident Response Guidelines, effective August 2001, document the Corporation's procedures for identifying and responding to security incidents. They define the types of incidents, the roles of organizational members (e.g., end users, the Information System Security Officer (ISSO), Computer Emergency Response Team, etc.), and its six stage structured approach to responding to computer security incidents. The Deputy Chief Information Officer is responsible for the external reporting to the Federal Computer Incident Response Center and the notification of the Corporation's Inspector General.

   **Procedures for external reporting to law enforcement authorities and to the General Services Administration's Federal Computer Incident Response Center (FedCIRC)**

   The guidelines state that the Deputy CIO and the ISSO will notify the Inspector General if there is evidence of criminal activity. There are no specific procedures contained within the guidelines related to how the Deputy CIO determines which events will be reported to FedCIRC.

   **Actual performance**

| | |
|---|---|
| a. Total number of agency components including bureaus, field activities. | 55 (field offices and services centers) |
| b. Number of agency components with incident handling and response capability. | Incident handling and response capabilities are centrally supported by CNS |

| | |
|---|---|
| | HQ OIT staff for all field offices and service centers that utilize the CNS LAN. |
| c. Number of agency components that report to FedCIRC. | 1 |
| d. Do the agency and its major components share incident information with FedCIRC in a timely manner consistent with FedCIRC and OMB guidance? | Per Corporation management there have been no incidents to report in FY02. |
| e. What is the required average time to report to the agency and FedCIRC following an incident? | 4 hours |
| f. How does the agency, including the programs within major components, confirm that patches have been tested and installed in a timely manner? | Corporation management states that patches are reviewed and tested prior to installation into the Production environment. |

| | FY01 | FY02 |
|---|---|---|
| g. By agency and individual component, 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 by each component | There were no successful intrusions.<br><br>There is no known requirement to maintain information related to the number and types of unsuccessful attempted intrusions.<br><br>If such a requirement were defined, the Corporation has stated it would comply. | There were no successful intrusions.<br><br>There is no known requirement to maintain information related to the number and types of unsuccessful attempted intrusions.<br><br>If such a requirement were defined, the Corporation has stated it would comply. |
| h. By agency and individual component, number of incidents reported externally to FedCIRC or law enforcement. | Per Corporation management, there were no reportable incidents. | Per Corporation management, there were no reportable incidents. |

## C. Responsibilities of Agency Program Officials

**1. Have agency program officials assessed the risk to operations and assets under their control, determined the level of security appropriate to protect such operations and assets, 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 tested and evaluated security controls and techniques?**

The Corporation relies on an independent contractor to periodically conduct risk assessments, to evaluate security controls and to update system security plans. Upon receipt of the contractor's reports, the Corporation re-accredits its systems. Such accreditation first occurred in 1997, and was re-performed in August 2001. In FY 2002, the Corporation's systems were not re-accredited; however, Corporation management has stated it intends to do so before December 31, 2002.

At the end of August 2002, a contractor began assessing the Corporation's systems, using the NIST Security Self-Assessment Guide methodology.

**Actual Performance**

| Corporation for National and Community Service | | | | |
|---|---|---|---|---|
| | FY01 | | FY02 | |
| Total Number of Agency Systems | 4 | | 5 | |
| | FY01 # | FY01 % | FY02 # | FY02 % |
| a. Systems that have been assessed for risk. | 4 | 100% | 4 | 80% |
| b. Systems that have been assigned a level of risk after a risk assessment has been conducted (e.g., high, medium, or basic). | 4 | 100% | 4 | 80% |
| c. Systems that have an up-to-date security plan. | 4 | 100% | 4 | 80% |
| d. Systems that have been authorized for processing following certification and accreditation. | 4 | 100% | 5 | 100% |
| e. Systems that are operating without written authorization (including the absence of certification and accreditation). | 0 | 0% | 0 | 0% |
| f. Systems that have the costs of their security controls integrated into the life cycle of the system. | 4 | 100% | 5 | 100% |
| g. Systems for which security controls have been tested and evaluated in the last year. | 4 | 100% | 4 | 100% |
| h. Systems that have a contingency plan. | 4 | 100% | 4 | 80% |

| | | | | |
|---|---|---|---|---|
| i. Systems for which contingency plans that have been tested in past year. | 4 | 100% | 4 | 80% |
| **AGENCY TOTAL** | 4 | 100% | 4 | 80% |

The 20% of the Corporation systems not tested in FY02 relates to the new e-Grants system that achieved limited operational status in June 2002. (See explanatory note on page 3 above.)

**2. Contractor Provided Services or Services Provided by Another Agency**

| Corporation for National And Community Service | | |
|---|---|---|
| | FY01 | FY02 |
| a. Number of contractor/agency operations or facilities. | 5 | 5 |
| b. Number of contractor/agency operations or facilities reviewed. | 5 | 5 |

Contractors and other government agencies:

- Aguirre Corporation/Interliant Inc.
- DOI National Business Center
- USDA National Finance Center
- Digex
- Sungard

## D. Responsibilities of Agency Chief Information Officer

**1. Has the agency CIO:**

**Adequately maintained an agency-wide security program;**

The lack of any security incidents or breaches in FY 2001 and FY 2002 indicates that at an operational level the Corporation has maintained effective security for its systems. However, it does not have security consistently integrated into planning, budgeting, documented procedures and routine testing as envisioned by GISRA legislation and regulation.

**Ensured the effective implementation of the program and evaluated the performance of major agency components;**

The Corporation has no components outside the headquarters facility with any significant IT capacity. The headquarters facility is small enough for the CIO to daily observe its operations.

**Ensured the training of agency employees with significant security responsibilities**

In addition to the security training that all CNS employees receive, information technology (IT) technical staff receive additional specialized security training according to job responsibilities and needs. They attend technical security training classes and conferences, and subscribe to on-line alert sources to further their knowledge of security and remain current with the rapidly evolving game of cat and mouse that information security has become. In 2002, six IT security specialists have attended specialized security training classes and conferences.

| | FY01 | FY02 |
|---|---|---|
| a. Other than GAO or IG audits and reviews, how many agency components and field activities received security reviews? | 55 | 55 |
| b. What percentage of components and field activities have had such reviews? | 100% through automated means. | 100% through automated means. |
| c. Number of agency employees including contractors. | Approx. 700 | Approx. 700 |
| Number and percentage of agency employees including contractors that received security training. | 100% | 100% |
| e. Number of employees with significant security responsibilities. | 5 | 6 |
| f. Number of employees with significant security responsibilities that received specialized training. | 5 | 6 |
| g. Briefly describe what types of security training were available. | Seminars, Classes, Conferences | Seminars, Classes, Conferences on Security and Information Assurance. |
| h. Total costs for providing training described in (g). | $10,000 | $12,000 |

The Corporation maintains its systems as a single entity which is composed of 55 locations. Since the IT resources for all locations are centrally provided, audits and reviews that are conducted are inclusive of all 55 locations.

| | |
|---|---|
| i. Do agency POA&Ms account for all known agency security weaknesses including all components and field activities? If no, why not? | The major findings from the IG's FY01 GISRA assessment were included on the Corporation's single POA&M. |
| j. Has the CIO appointed a senior agency information security official? | There is one Security Officer for the Corporation. |

All system users are required to receive system security training prior to being granted initial access to the Corporation's systems. In addition the Corporation maintains a database that records yearly participation in security training and disables user accounts if that training is not taken within the specified time period.

2. **Contractor Provided Services or Services Provided by Another Agency**

| | FY01 | FY02 |
|---|---|---|
| a. Number of contractor operations or facilities. | 5 | 5 |
| b. Number of contractor operations or facilities reviewed. | 5 Reviewed through automated means. | 5 Reviewed through automated means. |

Contractors and other government agencies:

- Aguirre Corporation/Interliant Inc.
- DOI National Business Center
- USDA National Finance Center
- Digex
- Sungard

3. **Has the agency CIO fully integrated security into the agency's capital planning and investment control process? Were security requirements and costs reported on every FY03 capital asset plan the exhibit 53 submitted by the agency to OMB.**

The Corporation did report estimated security costs as part of the FY 2003 exhibit 53 submission and again as part of the FY 2004 submission. In the budget submission itself only certain costs are specifically identified such as security training, accreditation/GISRA contracts and personnel. All other costs, such as security software, hardware and software maintenance are included under consolidated support items.

**Actual performance**

| | FY03 | FY04 |
|---|---|---|
| a. Number of capital asset plans and justifications submitted to OMB? | 4 | 4 |

| | | |
|---|---|---|
| b. Number of capital asset plans and justifications submitted to OMB without requisite security information and costs? | 0 | 0 |
| c. Were security costs reported for all agency systems on the agency's exhibit 53? | Yes | Yes |
| d. Have all discrepancies been corrected? | No | No |
| e. How many have the CIO/other appropriate official independently validated prior to submittal to OMB? | 4 | 4 |

# APPENDIX A

## Chart 1 - Overall GISRA Assessment Summary

| Control Objectives | Level1 Documented Policy | | | | | | | | Level 2 Documented Procedures | | | | | | | | Level 3 Implemented Procedures and Controls | | | | | | | | Level 4 Tested and Reviewed Procedures and Controls | | | | | | | | Level 5 Fully Integrated Procedures and Controls | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Momentum | | Agency Wide | | SPAN | | Network | | Momentum | | Agency Wide | | SPAN | | Network | | Momentum | | Agency Wide | | SPAN | | Network | | Momentum | | Agency Wide | | SPAN | | Network | | Momentum | | Agency Wide | | SPAN | | Network | |
| | '01 | '02 | '01 | '02 | '01 | '02 | '01 | '02 | '01 | '02 | '01 | '02 | '01 | '02 | '01 | '02 | '01 | '02 | '01 | '02 | '01 | '02 | '01 | '02 | '01 | '02 | '01 | '02 | '01 | '02 | '01 | '02 | '01 | '02 | '01 | '02 | '01 | '02 | '01 | '02 |
| **MANAGEMENT** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1. Risk Management | | | | | | | | | N | N | N | Y* | N | N | N | Y* | Y* | | Y* | Y* | Y* | Y* | Y* | Y* | | | | Y* | | | Y* | Y* | N | Y* | N | Y* | N | N | N | Y* |
| 2. Security Controls | | | | | | Y* | | | | Y* | | Y* | | Y* | | Y* | | Y* | | Y* | | Y* | Y* | Y* | Y* | Y* | | Y* | Y* | Y* | | Y* | Y* | Y* | Y* | Y* | Y* | Y* | N | Y* |
| 3. Life Cycle | | | | | | Y* | | | | Y* | | | | Y* | Y* | | Y* | | Y* | Y* | Y* | Y* | Y* | Y* | N | | N | Y* | N | Y* | N | Y* | N | | N | Y* | N | N | N | Y* |
| 4. Authorize Processing | | | | | | | | | | | | | | | | | Y* | | | | | | | | | | | | | | | | Y* | | | | | | N | |
| 5. Security Plan | | | | | | | | | | | | | | | | | | | Y* | | | | | | | | Y* | | | | | | N | Y* | N | | N | Y* | N | |
| **OPERATIONAL** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1. Personnel Security | Y* | | Y* | Y* | Y* | | Y* | Y* | Y* | Y* | Y* | Y* | Y* | Y* | Y* | Y* | Y* | Y* | Y* | Y* | Y* | Y* | Y* | Y* | | Y* | | | | Y* | | | Y* | Y* | Y* | Y* | Y* | Y* | N | Y* |
| 2. Physical Protection | | | | | | Y* | | | | Y* | Y* | Y* | Y* | Y* | | Y* | | | Y* | Y* | Y* | Y* | Y* | | Y* | | Y* | Y* | Y* | Y* | | Y* | Y* | Y* | N | Y* | N | Y* | N | Y* |
| 3. Production I/O | | | | | | Y* | | | | N | | | Y* | N | Y* | Y* | | | | | Y* | Y* | | Y* | | N | | | | N | | | | N | | | Y* | N | N | Y* |
| 4. Contingency Plan | | | | | | | | | | Y* | | Y* | | Y* | Y* | Y* | | Y* | | Y* | | Y* | | Y* | Y* | Y* | Y* | | Y* | Y* | Y* | | N | Y* | N | | N | Y* | N | Y* |
| 5. Hardware/Software | | Y* | | | | Y* | | | | Y* | | | Y* | Y* | | | | | | | Y* | | | | | | | | Y* | | | | | Y* | N | | N | Y* | N | |
| 6. Data Integrity | | | | | | | | | | | | | Y* | | | | | | | | Y* | | | | | | | | | | | | | | Y* | | Y* | | N | |
| 7. Documentation | | | | | | Y* | | | | | Y* | Y* | Y* | Y* | | | | | N | Y* | | | | | | | N | Y* | | | | | | Y* | N | Y* | Y* | Y* | N | |
| 8. Security Training | | | | | | | | | Y* | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | N | |
| 9. Incident Response | Y* | | Y* | | Y* | | Y* | | Y* | | Y* | | Y* | | Y* | | Y* | | Y* | | Y* | | Y* | | Y* | | Y* | | Y* | | Y* | | N | | N | | N | | N | |
| **TECHNICAL** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1. Authentication | | Y* | | | | Y* | | Y* | | | | | | Y* | | Y* | Y* | | Y* | Y* | Y* | Y* | Y* | Y* | | | | | | Y* | | | | | Y* | | Y* | N | Y* |
| 2. Logical Access | | | | | | | | | | | | Y* | | | | Y* | | | | | | | | | | | | | | | | | | Y* | | Y* | | | N | Y* |
| 3. Audit Trails | N | | | | | Y* | | | | | | | Y* | Y* | | | Y* | | | Y* | Y* | Y* | | | Y* | | Y* | | Y* | Y* | Y* | | N | | N | | N | N | N | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **OVERALL** | | Y* | | Y* | | | | Y* | Y* | Y* | Y* | Y* | Y* | Y* | Y* | Y* | Y* | Y* | Y* | Y* | Y* | Y* | Y* | Y* | Y* | Y* | Y* | Y* | Y* | Y* | Y* | Y* | N | Y* | N | Y* | N | Y* | N | Y* |

**Note on reading Chart 1**

In Chart 1 above, the CIO Council Framework Levels are shown as column headings with the individual Corporation assets that were evaluated shown diagonally below them. The NIST Guide's control criteria are shown as row headings. The control criteria fall into three general groupings: Management Controls, Operational Controls and Technical Controls.

In the main body of the charts a "Yes" means that the criteria for the specific control objective at the specific Framework Level were met. A "Yes*" means that some weaknesses were observed, but the criteria were generally met. A "No" means the criteria were not met in some significant respect. The chart has similar ratings shaded the same tone. The black areas are not relevant.

A similar chart in each of the following appendices shows the evaluation results for each system.

# APPENDIX B

# AGENCY-WIDE POLICIES AND PROCEDURES
# GISRA Assessment Summary
# FY 2002

## BACKGROUND

The Corporation for National and Community Service (CNS) maintains both WAN and LAN connections for its employees, contractors, and the classrooms of the AmeriCorps National Civilian Community Corps (NCCC). There are more than 800 computers in use on the CNS network. The Corporation's WAN connects LANs at the Corporation's regional service centers, NCCC campuses, and state offices with the Corporation's headquarters. Regional service centers have local network servers. However, the majority of the Corporation's network servers are located at Corporation headquarters in Washington, DC. These servers also provide email and Oracle services to the entire WAN. The Corporation has continuous connection to a disaster recovery site in Herndon, VA for immediate cut-over in case of an emergency. The Corporation's headquarters is connected to the disaster recovery site via a dedicated T1 line.

The Corporation uses Momentum as its financial management system. Momentum is an Oracle based proprietary system developed by AMS. The Web Based Reporting System (WBRS) is a Lotus Notes Domino program developed to help State commissions and other grantees provide financial and program status information to the Corporation. Momentum and WBRS are both managed at remote data centers. The System for Programs, Agreements, and National Service Participants (SPAN) is an Oracle based system used to manage the National Service Trust and to provide AmeriCorps member eligibility and service information.

The senior CNS official responsible for agency-wide information technology policies and procedures is the Chief Information Officer, Dave Spevacek.

The methodology used for this GISRA assessment is the CIO Council's Federal Information Security Self-Assessment Framework. The Self-Assessment Framework requires the use of the control criteria found in NIST Special Publication 800-26.

The remainder of this report summarizes the key strengths and weaknesses for management, operational, and technical controls. Each weakness is classified with a severity rating of major, medium or minor. Special weight was given to those areas that GISRA directly addresses.

## Chart 2 - Agency-Wide - GISRA Assessment Summary

| | Level1 | | | Level 2 | | | Level 3 | | | Level 4 | | | Level 5 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Documented Policy | | | Documented Procedures | | | Implemented Procedures and Controls | | | Tested and Reviewed Procedures and Controls | | | Fully Integrated Procedures and Controls | | |
| Control Objectives | FY01 | FY02 | | FY01 | FY02 | | FY01 | FY02 | | FY01 | FY02 | | FY01 | FY02 | |
| **MANAGEMENT** | | | | | | | | | | | | | | | |
| 1. Risk Management | YES | YES | | NO | YES* | Medium | YES* | YES* | Medium | YES | YES* | Medium | NO | YES* | Medium |
| 2. Security Controls | YES | YES | | YES | YES* | Medium | YES | YES* | Medium | YES | YES* | Medium | YES* | YES* | Medium |
| 3. Life Cycle | YES | YES | | YES | YES | | YES* | YES* | Minor | NO | YES* | Minor | NO | YES* | Minor |
| 4. Authorize Processing | YES | YES | | YES | YES | | YES | YES | | YES | YES | | YES | YES | |
| 5. Security Plan | YES | YES | | YES | YES | | YES* | YES | | YES* | YES | | NO | YES | |
| **OPERATIONAL** | | | | | | | | | | | | | | | |
| 1. Personnel Security | YES* | YES* | Minor | YES* | YES* | Minor | YES* | YES* | Minor | YES | YES | | YES* | YES* | Minor |
| 2. Physical Protection | YES | YES | | YES* | YES* | Medium | YES* | YES* | Medium | YES* | YES* | Medium | NO | YES* | Medium |
| 3. Production I/O | N/A | N/A | | N/A | N/A | | N/A | N/A | | N/A | N/A | | N/A | N/A | |
| 4. Contingency Plan | YES | YES | | YES | YES* | Medium | YES | YES* | Medium | YES* | YES | | NO | YES | |
| 5. Hardware/Software | YES | YES | | YES | YES | | YES | YES | | YES | YES | | NO | YES | |
| 6. Data Integrity | YES | YES | | YES | YES | | YES | YES | | YES | YES | | YES* | YES | |
| 7. Documentation | YES | YES | | YES* | YES* | Minor | NO | YES* | Minor | NO | YES* | Minor | NO | YES* | Minor |
| 8. Security Training | YES | YES | | YES | YES | | YES | YES | | YES | YES | | YES | YES | |
| 9. Incident Response | YES* | YES | | YES* | YES | | YES* | YES | | YES* | YES | | NO | YES | |
| **TECHNICAL** | | | | | | | | | | | | | | | |
| 1. Authentication | YES | YES | | YES | YES | | YES* | YES* | Medium | YES | YES | | YES | YES* | Medium |
| 2. Logical Access | YES | YES | | YES | YES* | Minor | YES | YES* | Minor | YES | YES | | YES | YES* | Minor |
| 3. Audit Trails | YES | YES | | YES | YES | | YES | YES | | YES* | YES | | NO | YES | |
| **OVERALL** | YES | YES* | | YES* | YES* | | YES* | YES* | | YES* | YES* | | NO | YES* | |

## A. MANAGEMENT CONTROLS

Strengths: In accordance with OMB Circular A-130, the CNS Computer Security Policy requires that risk assessments be conducted every three years or when major system changes occur. In conjunction with the re-accreditation process, risk analyses were conducted for all of CNS's mission critical systems and network in FY01. Similar re-accreditations began in August 2002. Corporation program officials are required to accept responsibility for the risks identified to mission critical systems and for the level of security provided to mitigate those risks. CNS has a documented security plan that identifies security related activities that are to be performed, their frequency, and the responsibilities for performance.

Weakness: CNS does not have documented procedures for conducting risk assessments. CNS relies upon the guidance in OMB Circular A-130 (severity: medium). The most recent risk assessments performed for the Corporation have not included a business impact analysis (severity: medium).

## B. OPERATIONAL CONTROLS

Strengths: Per the CNS computer security policy, user access is restricted based upon "a need to know". Users' access is restricted to only the information required to perform their jobs and as authorized by their supervisors. CNS requires that access request forms be completed and approved by management prior to granting an employee access to the CNS Network or applications. Background investigations are completed for all CNS employees.

Portable fire extinguishers are located in Corporation office spaces, and an automated fire suppression system is installed in the building. In the event of a power outage, the Corporation has an Uninterruptible Power Supply that will allow for the orderly shut down of the network. The CNS policy on "Safeguarding Sensitive Information and Documents" provides users with guidelines for storage, disposal and handling of sensitive information and documents.

Weakness: Risk assessments for Corporation facilities to identify threats, vulnerabilities and potential business impacts are not required by CNS's security policy. CNS relies upon the guidance in OMB Circular A-130 (severity: medium).

## C. TECHNICAL CONTROLS

Strengths: Access to the CNS network and applications is granted on a need-to-know basis. Users are not granted emergency or temporary access. All users must adhere to the CNS authentication policies and procedures. Users are required to obtain supervisory authorization to obtain access to applications residing on the CNS network.

Weakness: There is no policy or procedure that requires CNS users to use strong passwords (i.e. passwords with a combination of letters, numbers, and special characters). Periodically, IT security management uses security tools to detect user accounts with weak passwords. Users with weak passwords are instructed to modify their passwords immediately. The version of MS Windows currently on many of the workstations does not provide an automated method for central enforcement of strong passwords. The Corporation is in the process of upgrading the MS Windows software on all workstations. (severity: medium)

# APPENDIX C

# LOCAL AND WIDE AREA NETWORKS GISRA ASSESSMENT SUMMARY FY 2002

## BACKGROUND

The Corporation for National Service (CNS) Network consists of a local area network (LAN) in the headquarters office, with a high speed Frame-Relay network provided by MCI for remote Regional Service Centers, State Offices, National Civilian Community Corps (NCCC) campuses and remote processing sites. Web servers reside on the public side of the Corporation Network outside the headquarters firewall, and are provided by DigEx. A single high speed Internet connection through the firewall is provided for all Corporation users. Some dial-in service is provided for remote offices through a server-controlled modem pool. The Corporation's website, //http:www.cns.gov, is managed by Digex.

The Office of Information Technology (OIT) provides all administrative and problem support for IT equipment installed in remote offices. OIT monitors network vulnerabilities, maintains an intrusion detection capability on the network, and periodically performs its own penetration testing.

Mr. Tom Hanley, Deputy CIO, is the designated program official for the Corporation Network, and is responsible for overall network security.

The methodology used for this GISRA assessment is the CIO Council's Federal Information Security Self-Assessment Framework. The Self-Assessment Framework requires the use of the control criteria found in NIST Special Publication 800-26.

The remainder of this report summarizes the key strengths and weaknesses for management, operational, and technical controls. Each weakness is classified with a severity rating of major, medium or minor. Special weight was given to those areas that GISRA directly addresses.

## Chart 3 - Network - GISRA Assessment Summary

| | Level1 | | | Level 2 | | | Level 3 | | | Level 4 | | | Level 5 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Documented Policy | | | Documented Procedures | | | Implemented Procedures and Controls | | | Tested and Reviewed Procedures and Controls | | | Fully Integrated Procedures and Controls | | |
| Control Objectives | FY01 | FY02 | | FY01 | FY02 | | FY01 | FY02 | | FY01 | FY02 | | FY01 | FY02 | |
| **MANAGEMENT** | | | | | | | | | | | | | | | |
| 1. Risk Management | YES | YES | | NO | YES* | Medium | YES* | YES* | Medium | YES | YES* | Medium | NO | YES* | Medium |
| 2. Security Controls | YES | YES | | YES | YES* | Medium | YES | YES* | Medium | YES | YES* | Medium | YES* | YES* | Medium |
| 3. Life Cycle | YES | YES | | YES | YES | | YES* | YES* | Medium | NO | YES* | Medium | NO | YES* | Medium |
| 4. Authorize Processing | YES | YES | | YES | YES | | YES* | YES | | YES | YES | | YES* | YES | |
| 5. Security Plan | YES | YES | | YES | YES | | YES* | YES | | YES* | YES | | NO | YES | |
| **OPERATIONAL** | | | | | | | | | | | | | | | |
| 1. Personnel Security | YES* | YES* | Minor | YES* | YES* | Minor | YES* | YES* | Minor | YES | YES | | YES* | YES* | Minor |
| 2. Physical Protection | YES | YES | | YES* | YES* | Medium | YES* | YES | | YES* | YES* | Medium | NO | YES* | Medium |
| 3. Production I/O | N/A | YES | | N/A | YES* | Minor | N/A | YES* | Medium | N/A | YES | | N/A | YES* | Minor |
| 4. Contingency Plan | YES | YES | | YES | YES* | Minor | YES | YES* | Minor | YES* | YES | | NO | YES* | Minor |
| 5. Hardware/Software | YES | YES | | YES | YES | | YES | YES | | YES | YES | | NO | YES | |
| 6. Data Integrity | YES | YES | | YES | YES | | YES | YES | | YES | YES | | YES* | YES | |
| 7. Documentation | YES | YES | | YES* | YES | | NO | YES | | NO | YES | | NO | YES | |
| 8. Security Training | YES | YES | | YES | YES | | YES | YES | | YES | YES | | YES | YES | |
| 9. Incident Response | YES* | YES | | YES* | YES | | YES* | YES | | YES* | YES | | NO | YES | |
| **TECHNICAL** | | | | | | | | | | | | | | | |
| 1. Authentication | YES | YES* | Medium | YES | YES* | Medium | YES* | YES* | Medium | YES | YES | | YES | YES* | Medium |
| 2. Logical Access | YES | YES | | YES | YES* | Minor | YES | YES | | YES | YES | | YES | YES* | Minor |
| 3. Audit Trails | YES | YES | | YES | YES | | YES | YES | | YES* | YES | | NO | YES | |
| **OVERALL** | YES | YES* | | YES* | YES* | | YES* | YES* | | YES* | YES* | | NO | YES* | |

## A. MANAGEMENT CONTROLS

Strengths: A re-accreditation of the network was completed in February 2001 and is being performed again in FY02. Various monitoring tools have been enabled to identify and observe threats and vulnerabilities (i.e. vulnerability analyses and penetration testing are performed annually). Pro-active measures, such as required security awareness training, a virus protection program, access controls, and remote site network management are indications of management's day-to-day attention to security. CNS implemented a new System Development Life Cycle (SDLC) policy and methodology in August 2002.

CNS policy requires that each critical system have a system security plan. CNS has developed such a plan for the network. The corporation's security program, which includes the IT Network Security Plan, is included as an appendix to the Information Management Strategic Plan.

In mid-August 2002, the Corporation began a GISRA assessment in accordance with the NIST Security Self-Assessment methodology and the CIO Council's Federal Information Technology Security Assessment Framework using contractor personnel..

Weakness: CNS does not have documented procedures for conducting risk assessments. CNS relies upon the guidance in OMB Circular A-130 (severity: medium). The most recent risk assessments performed for the Corporation have not included a business impact analysis (severity: medium).

## B. OPERATIONAL CONTROLS

Strengths: Job descriptions within OIT reflect assigned responsibilities, include requirements for technical knowledge, skills and abilities, and can be used for performance evaluations. Access to systems is restricted prior to the completion of the new employee computer security training and supervisory approval. The computer room at CNS headquarters, which houses the majority of the network and server components, is a restricted access facility. Access is restricted to a limited number of authorized individuals. Visitors must sign in and be escorted by an authorized individual. All access is logged via the Kastle card key system. The computer room has an uninterruptible power supply that protects against power fluctuations and outages. A Disaster Recovery Plan was last updated in August 2001. CNS tested its Disaster Recovery Plan in August 2001 and advised that it plans to conduct another test in September 2002. Functional users participate in the disaster recovery testing to ensure the availability and accuracy of critical business applications and data. An ongoing security awareness program has been implemented. It includes first-time training for all new employees, contractors, and users, and periodic refresher training thereafter. A new version of the Computer Incident Response Guidelines was released August 2001. The

CNS Computer Incident Response Guidelines address the conditions and procedures for involving the CNS Inspector General (IG) or external federal authorities.

Weakness: Risk assessments for Corporation facilities to identify threats, vulnerabilities and potential business impacts are not required by CNS's security policy. CNS relies upon the guidance in OMB Circular A-130 (severity: medium). The Disaster Recovery Plan needs to be updated to reflect changes in the LAN environment (severity: medium).

## C. TECHNICAL CONTROLS

Strengths: All personnel who are given access to the system, including those needing it for a limited duration, must follow the standard procedures before being granted access. Logical access controls are in place for the local and remote network. In addition to controlling access to the network by users, CNS controls network access by port based on the MAC address of the PC or server. The Network Security Plan describes numerous checks that must be made of a variety of security controls, the frequency of the checks and who is responsible for making them. Review of various audit logs is included in the list.

Weakness: There is no policy or procedure that requires CNS users to use "strong" passwords (i.e. passwords with a combination of letters, numbers, and special characters). Periodically, IT security management uses security tools to detect user accounts with "weak" passwords. Users with "weak" passwords are instructed to modify their passwords immediately. The version of MS Windows currently on many of the workstations does not provide an automated method for central enforcement of strong passwords. However, the Corporation is in the process of upgrading the MS Windows software on all workstations (severity: medium).

During our penetration testing, procedures and policies that dictate how Administrator accounts are to be set-up were not followed. A server 'Administrator' account with a weak password was detected and compromised. In addition, some database accounts still had the software vendor's default passwords. These were also detected and compromised. When advised of these situations, the Corporation took prompt action to remedy them (severity: medium).

# APPENDIX D

# *MOMENTUM*
# *GISRA ASSESSMENT SUMMARY*
# *FY 2002*

## BACKGROUND

Momentum is the Corporation's financial management system. It was implemented in September 1999, and is comprised of 10 modules: Accounts Payable, Accounts Receivable, Automated Disbursements, Budget Execution, Cost Allocation, General Ledger, General System, Planning, Project Cost Accounting and Purchasing. The Momentum computers are located at the Department of Interior's National Business Center, but Corporation users have access Momentum as if it were a local system.

Momentum was developed by American Management Systems (AMS), who remains responsible for development, maintenance and configuration control of the application. Momentum hardware is operated for CNS at the Department of Interior (DOI) National Business Center (NBC) in Reston, Virginia. CNS has a Service Level Agreement with NBC. NBC in turn has a contract with AMS for maintenance of the Momentum software. The Momentum system is connected to the CNS LAN by a dedicated T-1 line.

Data in the Momentum application is critical to CNS financial management. Momentum provides both comprehensive financial planning capabilities and a means to record financial transactions. The system provides both detailed and summarized financial information in a multitude of easily understandable formats to enable users to evaluate and analyze the financial activities.

The "senior program official" in CNS responsible for Momentum is Gerry Yetter, Director of Accounting. Wynn Cooper, Financial Systems Team Lead, assists Gerry Yetter.

The methodology used for this GISRA assessment is the CIO Council's Federal Information Security Self-Assessment Framework. The Self-Assessment Framework requires the use of the control criteria found in NIST Special Publication 800-26.

The remainder of this report summarizes the key strengths and weaknesses for management, operational, and technical controls. Each weakness is classified with a severity rating of major, medium or minor. Special weight was given to those areas that GISRA directly addresses..

## Chart 4 - Momentum - GISRA Assessment Summary

| | Level1 | | | Level 2 | | | Level 3 | | | Level 4 | | | Level 5 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | Implemented Procedures | | | Tested and Reviewed | | | Fully Integrated | | |
| | Documented Policy | | | Documented Procedures | | | and Controls | | | Procedures and Controls | | | Procedures and Controls | | |
| Control Objectives | FY01 | FY02 | | FY01 | FY02 | | FY01 | FY02 | | FY01 | FY02 | | FY01 | FY02 | |
| **MANAGEMENT** | | | | | | | | | | | | | | | |
| 1. Risk Management | YES | YES | | NO | NO | Medium | YES* | YES | | YES | YES | | NO | YES* | Medium |
| 2. Security Controls | YES | YES | | YES | YES* | Medium | YES | YES* | Medium | YES* | YES* | Medium | YES* | YES* | Medium |
| 3. Life Cycle | YES | YES | | YES | YES* | Minor | YES* | YES | | NO | YES | | NO | YES | |
| 4. Authorize Processing | YES | YES | | YES | YES | | YES* | YES | | YES | YES | | YES* | YES | |
| 5. Security Plan | YES | YES | | YES | YES | | YES* | YES | | YES | YES | | NO | YES* | Minor |
| **OPERATIONAL** | | | | | | | | | | | | | | | |
| 1. Personnel Security | YES* | YES | | YES* | YES* | Medium | YES* | YES* | Medium | YES | YES* | Medium | YES* | YES* | Medium |
| 2. Physical Protection | YES | YES | | YES | YES* | Medium | YES | YES | | YES* | YES | | YES* | YES* | Medium |
| 3. Production I/O | YES | YES | | YES | NO | Minor | YES | YES | | YES | NO | Minor | YES | NO | Minor |
| 4. Contingency Plan | YES | YES | | YES | YES* | Medium | YES | YES* | Medium | YES* | YES* | Medium | NO | YES* | Medium |
| 5. Hardware/Software | YES | YES* | Medium | YES | YES* | Medium | YES | YES | | YES | YES | | YES | YES* | Medium |
| 6. Data Integrity | YES | YES | | YES | YES | | YES | YES | | YES | YES | | YES | YES | |
| 7. Documentation | YES | YES | | YES | YES | | YES | YES | | YES | YES | | YES | YES* | Medium |
| 8. Security Training | YES | YES | | YES* | YES | | YES | YES | | YES | YES | | YES | YES | |
| 9. Incident Response | YES* | YES | | YES* | YES | | YES* | YES | | YES* | YES | | NO | YES | |
| **TECHNICAL** | | | | | | | | | | | | | | | |
| 1. Authentication | YES | YES* | Minor | YES | YES | | YES* | YES | | YES | YES | | YES | YES | |
| 2. Logical Access | YES | YES | | YES | YES | | YES | YES | | YES | YES | | YES | YES* | Minor |
| 3. Audit Trails | NO | YES | | YES | YES | | YES* | YES | | YES* | YES | | NO | YES | |
| **OVERALL** | YES | YES* | | YES* | YES* | | YES* | YES* | | YES* | YES* | | NO | YES* | |

## A. MANAGEMENT CONTROLS

Strengths: As part of the re-accreditation of Momentum, data sensitivity and integrity were considered. CNS maintains a system security plan for the Momentum application, consistent with the CNS Computer Security Policy. The security plan was developed in accordance with NIST 800-18 guidance. Physical safeguards have been established that are commensurate with the risks of physical damage or access. Security controls for CNS's mission critical systems, which include Momentum, have been reviewed every three years in accordance with OMB A-130 re-accreditation requirements. Procedures for reporting security incidents and weaknesses are in place and linked to the risk management process.

Weakness: CNS does not have documented procedures for conducting risk assessments. CNS relies upon the guidance in OMB Circular A-130 (severity: medium). The most recent risk assessments performed for the Corporation have not included a business impact analysis (severity: medium). There is no documented procedure for the periodic review of the operating system's configuration (severity: medium). There is no documented procedure for determining the sensitivity of the system (severity: minor). There is no documented procedure for developing and approving a system security plan (severity: minor).

## B. OPERATIONAL CONTROLS

Strengths: CNS's computer security policy is based on the concept of least privilege, which requires that users only have access to that information that they require to perform their job function. Access is limited to individuals at CNS through the use of identification badges and key cards. Data integrity and validation controls are used to provide assurance that the information has not been altered and the system functions as intended. Controls have been implemented to mitigate other disasters such as floods, earthquakes or fire. CNS has updated and tested its disaster recovery plan in August 2001. A Service Level Agreement exists with the National Business Center (NBC) that calls for NBC to provide monitoring, maintenance and tracking of configuration changes for the hardware, system software, database software and telecommunications. Corporation employees and contractors are required to complete annual security awareness training. Training requires all CNS IT users to acknowledge rules and guidelines by which they must abide. CNS has documented and updated Computer Incident Response Guidelines specifying internal reporting procedures for detected security incidents.

Weakness: The Business Continuity and Contingency plan dated August 2001 was prepared initially for Y2K. No significant changes have been made to it. However, the Corporation does conduct annual tests of its Disaster Recovery Plan. The next testing is scheduled for September 2002 (severity: medium). No documented procedure exists for management review of persons granted physical access to sensitive facilities. However,

the Deputy CIO does review the names on the computer center sign-in roster to ensure that only authorized persons have been granted access (severity: medium). No documented policy and procedure exists to ensure that access to all program libraries is restricted and controlled (severity: medium). No documented analysis has been completed to assess risks (severity: medium). CNS does not have documented procedures for personnel security controls that meet the NIST criteria (severity: medium).

## C. TECHNICAL CONTROLS

Strengths: All CNS users are required to identify and authenticate themselves by providing a valid username and password at the network level. CNS users who have been granted access to Momentum are required to authenticate to the application by providing an additional user name and password. All Momentum users are required to undergo annual Information Systems Security Awareness Training that educates them on the importance of security. Every transaction processed in Momentum is written to the transaction journal. Because all transactions are recorded in a journal, there is a comprehensive audit trail of all transaction-based activity in the system.

Weakness: No documented policies exist to limit the number of invalid access attempts (severity: minor). Although data owners do review access authorizations, there is no policy that requires the data owners to periodically review access authorization (severity: minor). Some CNS user workstations do not automatically log off users and invoke screensavers after a period of inactivity of a defined length, because the version of MS Windows currently on these systems is not capable of implementing the automatic logout feature. The Corporation is in the process of upgrading all workstations to a newer version of MS Windows (severity: minor).

# APPENDIX E

# SYSTEM FOR PROGRAMS, AGREEMENTS AND NATIONAL SERVICE PARTICIPANTS (SPAN) GISRA ASSESSMENT SUMMARY FY 2002

## BACKGROUND

The SPAN application was implemented in 1995 to process education award payments for the AmeriCorps National Service Program. The VISTA Management System (VMS), integrated into SPAN in March 2001, tracks the status of and makes payments to participants of the Volunteers in Service to America (VISTA) program. Three dedicated Windows NT servers within the Corporation Network provide separate production, development, and testing platforms for SPAN. SPAN is based on an Oracle database management system, and was developed using Oracle application development tools, Oracle Forms for data entry screens, Crystal Report Writer and Oracle Reports for report generation. SQL SECURE Password Manager by BrainTree provides authentication and access security to SPAN.

SPAN interfaces with Momentum, WBRS, and the Department of the Treasury. Weekly file uploads to Momentum update Corporation accounting data. SPAN uses electronic file transfers to receive enrollment data from WBRS, and to provide updated financial information to WBRS. For the Treasury interface, a SPAN export function creates a payment file, which is electronically transmitted to Treasury from a stand-alone workstation using Treasury software. There is no direct connection between SPAN and Treasury's financial management system.

The senior Corporation program official responsible for SPAN is Charlene Dunn, Director of Trust Management.

The methodology used for this GISRA assessment is the CIO Council's Federal Information Security Self-Assessment Framework. The Self-Assessment Framework requires the use of the control criteria found in NIST Special Publication 800-26.

The remainder of this report summarizes the key strengths and weaknesses for management, operational and technical controls. Each weakness is classified with a severity rating of major, medium or minor. Special weight was given to those areas that GISAR directly addresses.

## Chart 5 - SPAN - GISRA Assessment Summary

| Control Objectives | Level 1 Documented Policy | | | Level 2 Documented Procedures | | | Level 3 Implemented Procedures and Controls | | | Level 4 Tested and Reviewed Procedures and Controls | | | Level 5 Fully Integrated Procedures and Controls | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | FY 01 | FY 02 | | FY 01 | FY 02 | | FY 01 | FY 02 | | FY 01 | FY 02 | | FY 01 | FY 02 | |
| **MANAGEMENT** | | | | | | | | | | | | | | | |
| 1. Risk Management | YES | YES | | NO | NO | | YES* | YES* | Medium | YES | YES | | NO | NO | Medium |
| 2. Security Controls | YES | YES* | Minor | YES | YES* | Medium | YES | YES* | Medium | YES* | YES* | Medium | YES* | YES* | Medium |
| 3. Life Cycle | YES | YES* | Medium | YES | YES* | Medium | YES* | YES* | Medium | NO | YES* | Medium | NO | NO | Medium |
| 4. Authorize Processing | YES | YES | | YES | YES | | YES | YES | | YES | YES | | YES | YES | |
| 5. Security Plan | YES | YES | | YES | YES | | YES | YES | | YES | YES | | NO | YES* | Minor |
| **OPERATIONAL** | | | | | | | | | | | | | | | |
| 1. Personnel Security | YES* | YES | | YES* | YES* | Medium | YES* | YES* | Medium | YES | YES* | Medium | YES* | YES* | Medium |
| 2. Physical Protection | YES | YES* | Minor | YES* | YES* | Minor | YES* | YES* | Minor | YES* | YES* | Minor | NO | YES* | Minor |
| 3. Production I/O | YES | YES* | Minor | YES* | NO | Minor | YES* | YES* | Minor | YES | NO | Minor | YES* | NO | Minor |
| 4. Contingency Plan | YES | YES | | YES | YES* | Medium | YES | YES* | Medium | YES* | YES* | Medium | NO | YES* | Medium |
| 5. Hardware/Software | YES | YES* | Medium | YES* | YES* | Medium | YES* | YES | | YES* | YES | | NO | YES* | Medium |
| 6. Data Integrity | YES | YES | | YES* | YES | | YES* | YES | | YES | YES | | YES* | YES | |
| 7. Documentation | YES | YES* | Medium | YES* | YES* | Medium | YES | YES | | YES | YES | | YES* | YES* | Medium |
| 8. Security Training | YES | YES | | YES | YES | | YES | YES | | YES | YES | | YES | YES | |
| 9. Incident Response | YES* | YES | | YES* | YES | | YES* | YES | | YES* | YES | | NO | YES | |
| **TECHNICAL** | | | | | | | | | | | | | | | |
| 1. Authentication | YES | YES* | Minor | YES | YES* | Minor | YES* | YES* | Minor | YES | YES* | Minor | YES | YES* | Minor |
| 2. Logical Access | YES | YES | | YES | YES | | YES | YES | | YES | YES | | YES | YES | |
| 3. Audit Trails | YES | YES* | Minor | YES* | YES* | Minor | YES* | YES* | Minor | YES* | YES* | Minor | NO | NO | Minor |
| **OVERALL** | YES | YES | | YES* | YES* | | YES* | YES* | | YES* | YES* | | NO | YES* | |

## A. MANAGEMENT CONTROLS

Strengths: A risk analysis was conducted as part of the SPAN re-accreditation process, and is included as part of the accreditation document. The re-accreditation was completed in June 2001. CNS has developed and implemented a security plan for the SPAN application, in accordance with the CNS Computer Security Policy. The SPAN Security Plan states that the CNS System Development Life Cycle (SDLC) process was followed for the implementation, development, and operation/maintenance phase of the SPAN life cycle. The SPAN Security Plan also states that the IT Security Representative was heavily involved with the recent integration of VMS into SPAN.

Weaknesses: CNS does not have documented procedures for conducting risk assessments. CNS relies upon the guidance in OMB Circular A-130 (severity: medium). The most recent risk assessments performed for the Corporation have not included a business impact analysis (severity: medium). There is no documented procedure for periodically reviewing the operating system's configuration (severity: medium). There are no documented policies and procedures for ensuring electronic records are properly disposed or archived. (severity: minor).

## B. OPERATIONAL CONTROLS

Strengths: CNS computer security policy is based on the concept of least privilege, which requires that users only be granted access to that information that they require to perform their job function. Access is limited to individuals at CNS through the use of identification badges and key cards. Data integrity and validation controls are used to provide assurance that the information has not been altered and the SPAN system functions as intended. Controls have been implemented to mitigate other disasters such as floods, earthquakes or fire. CNS updated and tested its disaster recovery plan in August 2001. Corporation employees and contractors are required to complete annual security awareness training. Training requires all CNS IT users to acknowledge rules and guidelines by which they must abide. CNS has documented and updated Computer Incident Response Guidelines specifying internal reporting procedures for detected security incidents.

Weaknesses: The Business Continuity and Contingency plan dated August 2001 was prepared initially for Y2K. No significant changes have been made to it. However, the Corporation does conduct annual tests of its Disaster Recovery Plan. The next testing is scheduled for September 2002 (severity: medium). There are no documented policies and procedures regarding how data is shared between interconnected systems (severity: medium). There is no documented analysis completed to access risks (severity: medium). CNS has incomplete documented procedures for personnel security controls (severity: medium).

## C. TECHNICAL CONTROLS

Strengths: CNS users who have been granted access to SPAN are required to authenticate to the application by providing an additional user name and password in addition to their network username and password. All SPAN users are required to undergo annual Information Systems Security Awareness Training that educates users on the importance of security. Because every transaction processed in SPAN is written to a journal, there is a comprehensive audit trail of all transaction-based activity in the system.

Weaknesses: No documented policies exist to limit the number of invalid access attempts (severity: minor). Although data owners do review access authorizations, there is no policy that requires the data owners to periodically review access authorization (severity: minor). Some CNS user workstations do not automatically log off users and invoke screensavers after a period of inactivity of a defined length, because the version of MS Windows currently on these systems is not capable of implementing the automatic logout feature. The Corporation is in the process of upgrading all workstations to a newer version of MS Windows (severity: minor).