OFFICE OF THE INSPECTOR GENERAL
CORPORATION FOR NATIONAL AND COMMUNITY SERVICE

OIG Letter Report Regarding
Corporation For National and Community Service
Compliance With
The Government Information Security Reform Act

OIG Report Number 02-04
September 26, 2001

FOR OFFICIAL USE ONLY

This letter report contains information about Corporation computer security practices and vulnerabilities. All recipients of this report should take care to prevent the unauthorized disclosure of the report or its contents. Requests for release of this report or its contents must be referred to the Inspector General.

GSA Contract No. GS-23F-8127H
Purchase Order No. 200106210003
Task Order No. 00-01

This letter report was issued to Corporation management on October 5, 2001. Under OMB's implementing guidance, the Corporation must provide a plan of action and milestones to address identified security weaknesses by October 31, 2001, and thereafter provide quarterly status updates on remedial efforts. Additionally, OIG is required under GISRA to conduct follow-up evaluations in 2002. Weaknesses and corrective actions contained in this report will be included in the audit resolution process. The Corporation must make final management decisions no later than April 3, 2002 and complete its corrective actions by October 5, 2002.

Letter Report Regarding Compliance With The Government Information Security Reform Act OIG Report Number 02-04

CORPORATION
FOR NATIONAL
SERVICE

In compliance with section 3535 of Title 44, US Code, as added by the Government Information Security Reform Act of 2000 (Public Law 106-398), CNS OIG performed independent evaluations of the Corporation's information security program and practices and its compliance with the Act. In performing these evaluations, OIG followed implementing guidance and reporting instructions contained in two memorandums (M-01-08 and M-01-24) that the Office of Management and Budget issued on January 16, 2001 and June 22, 2001, respectively.

Between June and September 2001, OIG engaged KPMG LLP to analyze four elements of the Corporation's information technology systems, including:

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

For its analysis and related testing, KPMG used the CIO Council's "Federal Information Technology Security Assessment Framework" and the NIST "Security Self-Assessment Guide for Information Technology Systems" consistent with OMB's guidelines.

The assessments generally concluded that the Corporation has done a very respectable job of providing agency-wide information security but noted two areas that need improvement:

- Strengthening program officials' involvement in assessing security risks, understanding business impacts, and evaluating mitigating security measures
- Formally integrating security planning with overall information technology and business strategies and with resource allocation decision making

The CIO staff reviewed and commented on drafts of the four assessments (Appendices A through D) attached to this letter report.

Because this report concerns Corporation computer security practices and vulnerabilities, its distribution is limited to the Office of Inspector General and those management and CIO personnel of the Corporation who have a need to know the information in order to perform their official duties. It is also available upon request to the Office of Management and Budget and the United States Congress. Due to the sensitivity of its content, this report is exempt from release to the general public.

Office of Inspector General
Corporation for National and Community Service's
Letter Report Regarding Compliance With
The Government Information Security Reform Act

Table of Contents

2001 M Street, N.W.
Washington, D.C. 20036

September 26, 2001

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

At your request, KPMG LLP (KPMG) performed an evaluation of the Corporation for National 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 Memorandums M-01-08 and M-01-24. 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. Our evaluation used the CIO Council's Federal Information Technology Security Assessment Framework along with the corollary guidance, Special Publication 800-26, issued by the Department of Commerce, National Institute of Standards and Technology (NIST), as required by OMB. 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

In general we found that the Corporation does a very respectable job of providing agency-wide information security. It has a proactive staff, and management who understand the importance of information security to the conduct of the Corporation's business. It is strongest in its day to day operation and maintenance of the information security infrastructure and in its personnel security awareness and training program.

The areas that need improvement (listed below) tend to be those that that stem from new GISRA requirements:

- There should be strengthened involvement of program officials in assessing the security risks to their program areas, in understanding the possible business impacts and in evaluating the adequacy of the mitigating security measures that are in place.
- At present, information security planning principally has an operational focus, and is not forward looking. GISRA requires that security planning be formally integrated with overall information technology and business strategies and with resource allocation processes.

- GISRA places a premium on documentation of information security policies and procedures, as well as, actual performance of the procedures. Two areas specifically need improvement in the degree of documentation:

    - System development life cycle (SDLC) processes, and
    - Routine, periodic review of information security controls and audit logs to assure that the reviews are actually being accomplished.

Project Objectives

The objectives of this project 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 and implementing guidance from OMB.

Methodology

OMB Memorandum 01-24 requires the use of the CIO Council's "Federal Information Technology Security Assessment Framework" (The Framework). Coupled with the NIST "Security Self-Assessment Guide for Information Technology Systems", NIST Special Publication 800-26 (The NIST Guide), the Framework provides 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 can be compared.

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 Framework in the following four areas:

- 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) was not re-evaluated at this time, since it was assessed in conjunction with the recent audit of the Corporation's Financial Statement for Fiscal Year 2000.

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. More specifically, we attempted to simulate a number of security penetration scenarios. The results of this assessment were generally favorable.

The results of the evaluations that were done using the Framework's methodology are summarized in Appendices A through D. Chart 1 on the next page shows the results for all four evaluations. The 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 chart 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.

Appendix E contains suggested responses to the thirteen questions that OMB Memorandum 01-24 requested the Inspector Generals to answer. The suggested responses are based on the evaluations that were done, but there is not a direct one for one correlation.

Chart 1 - GISRA Assessments 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
MANAGEMENT																				
1. Risk Management					No	No	No	No	Yes*	Yes*	Yes*	Yes*				Yes*	No	No	No	No
2. Security Controls												Yes*	Yes*		Yes*		Yes*	Yes*	Yes*	No
3. Life Cycle								Yes*	Yes*	Yes*	Yes*	Yes*	No	No	No	No	No	No	No	No
4. Authorize Processing									Yes*								Yes*			No
5. Security Plan										Yes*				Yes*			No	No	No	No
OPERATIONAL																				
1. Personnel Security	Yes*	Yes*	Yes*	Yes*	Yes*	Yes*	Yes*	Yes*	Yes*	Yes*	Yes*	Yes*					Yes*	Yes*	Yes*	No
2. Physical Protection						Yes*	Yes*			Yes*	Yes*	Yes*	Yes*	Yes*	Yes*		Yes*	No	No	No
3. Production I/O							Yes*	Yes*			Yes*								Yes*	No
4. Contingency Plan								Yes*					Yes*	Yes*	Yes*	Yes*	No	No	No	No
5. Hardware/Software							Yes*				Yes*				Yes*			No	No	No
6. Data Integrity							Yes*				Yes*							Yes*	Yes*	No
7. Documentation						Yes*	Yes*			No				No				No	Yes*	No
8. Security Training					Yes*															No
9. Incident Response	Yes*	Yes*	Yes*	Yes*	Yes*	Yes*	Yes*	Yes*	Yes*	Yes*	Yes*	Yes*	Yes*	Yes*	Yes*	Yes*	No	No	No	No
TECHNICAL																				
1. Authentication									Yes*	Yes*	Yes*	Yes*								No
2. Logical Access																				No
3. Audit Trails	No						Yes*		Yes*		Yes*		Yes*	Yes*	Yes*	Yes*	No	No	No	No
OVERALL					Yes*	Yes*	Yes*	Yes*	Yes*	Yes*	Yes*	Yes*	Yes*	Yes*	Yes*		No	No	No	No

*****

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

APPENDIX A

OFFICE OF INSPECTOR GENERAL
CORPORATION FOR NATIONAL AND COMMUNITY SERVICE

AGENCY-WIDE POLICIES AND PROCEDURES
GISRA ASSESSMENT SUMMARY

BACKGROUND

The Corporation for National 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 approximately 800 computers on this network. The Corporation's WAN connects LANs at the Corporation's five regional service centers, five NCCC campuses, and several 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 a disaster recovery site in Herndon, VA, to which headquarters is connected via a dedicated T1 line.

Momentum is the Corporation's financial management system. It is an Oracle based proprietary system developed by AMS. 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 information. The Web Based Reporting System (WBRS) is a Lotus Notes Domino program developed to help both AmeriCorps programs and the state commissions that transmit Corporation supplied grant funds to many sub-recipients in each state, and to provide financial and program information to the Corporation. Momentum and WBRS are outsourced and operate at remote data centers. The U.S. Department of Agriculture, National Finance Center provides payroll processing for the Corporation.

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

ASSESSMENT OVERVIEW

CNS does a very respectable job of providing agency-wide information security. It has proactive staff and management who understand the need for information security, and give it priority. It is strongest in its day to day operation and maintenance of the information security infrastructure and in its personnel security awareness and training program.

The areas in which it needs improvement tend to be those that are new requirements stemming from GISRA. CNS has begun to involve senior program officials in assessing the information security risks to their program areas and the mitigating security measures that are in place. But, the extent of program official involvement is still limited, as is the assessment of business risks and impacts.

Information security planning has principally an operational focus, and is not yet forward looking, nor integrated with overall information technology and business strategies. Documented procedures are not yet established for the timely reporting of security incidents to the Office of Inspector General and to external authorities, as required by GISRA. The CIO acknowledges the requirement to update the reporting guidelines to comply with GISRA and is in the process of completing that task. In the interim, the CIO has indicated they will report security incidents to the OIG and appropriate external authorities.

Informality is preferred in many CNS processes, and there is relatively less documentation than there would be in a larger agency. This occurs primarily because of the limited number of information technology staff and overall resource constraints. Two areas specifically need improvement in the degree of documentation: 1) system life cycle development processes, and 2) the routine, periodic reviews of information security controls and audit logs to assure that the reviews are actually being accomplished.

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 following table summarizes the results of the assessment that was done based on the above standards and criteria. The remainder of this report summarizes the key strengths and weaknesses for each of the major control objectives. Each weakness is classified into a high, medium and low severity rating. Special weight was given to those areas that are directly addressed by the GISRA legislation.

ASSESSMENT RATINGS SUMMARY

	Level 1	Level 2	Level 3	Level 4	Level 5
Control Criteria	Documented Policy	Documented Procedures	Implemented Procedures and Controls	Tested and Reviewed Procedures and Controls	Fully Integrated Procedures and Controls
OVERALL	Yes	Yes*	Yes*	Yes*	No
MANAGEMENT					
1. Risk Management	Yes	No	Yes*	Yes	No
2. Security Controls	Yes	Yes	Yes	Yes	Yes*
3. Life Cycle	Yes	Yes	Yes*	No	No
4. Authorize	Yes	Yes	Yes	Yes	Yes
5. Security Plan	Yes	Yes	Yes*	Yes*	No
OPERATIONAL					
1. Personnel Security	Yes*	Yes*	Yes*	Yes	Yes*
2. Physical Protection	Yes	Yes*	Yes*	Yes*	No
3. Production I/O	n/a	n/a	n/a	n/a	n/a
4. Contingency Plan	Yes	Yes	Yes	Yes*	No
5. Hardware/Software	Yes	Yes	Yes	Yes	No
6. Data Integrity	Yes	Yes	Yes	Yes	Yes*
7. Documentation	Yes	Yes*	No	No	No
8. Training	Yes	Yes	Yes	Yes	Yes
9. Incident Response	Yes*	Yes*	Yes*	Yes*	No
TECHNICAL					
1. Authentication	Yes	Yes	Yes*	Yes	Yes
2. Logical Access	Yes	Yes	Yes	Yes	Yes
3. Audit Trails	Yes	Yes	Yes	Yes*	No

* some weaknesses observed

A. MANAGEMENT CONTROLS

1. RISK MANAGEMENT

Level 1	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
Yes	**No**	**Yes***	**Yes**	**No**

* some weaknesses observed

Strengths: In accordance with OMB Circular A-130, CNS's Computer Security policy requires that risk assessments be conducted every three years or when major system changes occur. This year, in conjunction with the re-accreditation process, risk analyses were conducted for all of CNS's mission critical systems and network.

CNS has implemented a new procedure that requires agency program officials to formally accept the responsibility for the risks identified to mission critical systems and for the level of security provided to mitigate those risks.

Weaknesses: CNS does not have a documented risk assessment procedure or methodology. The CNS policy does not provide guidance for integrating system risk management with program management. Program officials have not been formally responsible for the levels of risk and mitigation within the systems that support CNS's major programs. One of the consequences is that the system risk analyses that were recently done do not address specific business impacts. (severity: medium)

2. REVIEW OF SECURITY CONTROLS

Level 1	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
Yes	**Yes**	**Yes**	**Yes**	**Yes***

* some weaknesses observed

Strengths: Security controls for CNS's mission critical systems are reviewed and tested every three years in conjunction with the re-accreditation process. For 2001, the accreditation was limited to one year as CNS shifts to an annual accreditation program. The CNS Security Plan details various security controls, the frequency with which they should be reviewed and assigns responsibility for their review. CNS's computer security policy and procedures, also require that security incidents be analyzed and remedial actions taken.

Weaknesses: A GISRA assessment in accordance with the CIO Council's Federal Information Technology Security Assessment Framework was not done as required by OMB. Corporation policies have not yet been updated to be in accordance with the GISRA requirement for annual assessments. (severity: low)

3. Life Cycle

Level 1	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
Yes	**Yes**	**Yes***	**No**	**No**

* some weaknesses observed

Strengths: CNS has a documented policy and procedures for Life Cycle Management of systems.

Weaknesses: There is very little documentation to show that life cycle procedures are followed. Management states that the life cycle procedures are followed informally. Periodic review and testing of life cycle procedures is not done, nor required by CNS policies. (severity: medium)

4. Authorize Processing (Certification and Accreditation)

Level 1	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
Yes	**Yes**	**Yes**	**Yes**	**Yes**

Strengths: In accordance with CNS policies, all of CNS's mission critical application systems were formally re-accredited in June 2001. During the re-accreditation process a security evaluation and risk assessment were completed, and a security plan developed for the system.

Weaknesses: None Observed.

5. System Security Plan

Level 1	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
Yes	**Yes**	**Yes***	**Yes***	**No**

* some weaknesses observed

Strengths: CNS has a documented security plan that identifies security related activities, the time frame in which they are to be performed and the individuals or groups that are responsible for performing the activities.

Weaknesses: CNS's agency-wide security plan details routine operational actions, but is not forward looking. It does not describe a strategy for providing security to all of CNS's systems and network, nor does it address how future deadlines for implementing security requirements that are mandated by current legislation will be met. For instance, it does not describe the steps the Corporation plans to take to comply with the Government Paperwork Elimination Act (GPEA). A summary of CNS's security plans is not included in the IT strategic plan as required by GISRA. (severity: medium)

B. OPERATIONAL CONTROLS

1. Personnel Security

Level 1	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
Yes*	**Yes***	**Yes***	**Yes**	**Yes***

* some weaknesses observed

Strengths: CNS's computer security policy is based on the concept of least privilege. Users are granted access only to the information they need to perform their job.

CNS requires that an Information System Access request form be approved by management prior to an employee being granted access to a CNS Information System.

The Corporation does not have a written policy regarding personnel screening of its employees. The Human Resources Office reports that it requests a National Agency Check on certain employees serving in certain selected positions after they are hired.

Documented job descriptions exist for employees of the CNS Office of Information Technology (OIT). Security responsibilities for the CIO and Information Systems Security Officer are also documented in the CNS Network Security Plan.

Users of CNS information systems are advised of their rights and responsibilities through the Network logon banner, security awareness training and the CNS Policy "Internet and E-mail Access and Acceptable Use".

Weaknesses: Corporation security procedures for employee and contractor terminations are not documented. Even for unfriendly terminations the procedures are informal and depend on particular individuals being aware of each specific situation. (severity: low)

CNS has a small IT staff. The separation of duties is not specifically documented, and is not as much as it would be in a larger organization. But, CNS management feels that there is about as much separation of duties as is practical. (severity: low)

2. PHYSICAL AND ENVIRONMENT PROTECTION

Level 1	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
Yes	**Yes***	**Yes***	**Yes***	**No**

* some weaknesses observed

Strengths: Access to the Corporation's Computer Room - Data Center is restricted. No employees are permanently assigned to be in the Data Center, and all visitors to the Data Center are required to sign in, in accordance with the CNS security policy.

Access to general office space is controlled by electronic access keys. Receptionists control access for those without access keys.

In the event of a power outage, the Corporation has an Uninterruptible Power Supply that will allow it time to do an orderly shut down of its systems. Portable fire extinguishers are available in Corporation office spaces, and an automated fire suppression system is installed in the building.

Weaknesses: Risk assessments for Corporation facilities to identify threats, vulnerabilities and potential business impacts are not required by CNS's security policy nor done on a periodic basis. (severity: low) OIG has previously reported weak accountability for the electronic access keys and for the master keys that control access to every floor. There are no documented requirements or procedures for securing unused keys. (severity: medium) Reception personnel do not consistently challenge visitors. (severity: low)

3. Production Input/ Output Controls

Level 1	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
n/a	**n/a**	**n/a**	**n/a**	**n/a**

Strengths: For systems that CNS operates on its own behalf, users of the system control all input and output. There is no central operations staff at CNS. CNS also has two systems whose operation is out-sourced to other service providers. In these cases too, input and output is controlled by the system users.

Weaknesses: None observed.

4. Contingency Planning

Level 1	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
Yes	**Yes**	**Yes**	**Yes***	**No**

* some weaknesses observed

Strengths: CNS has a documented business continuity plan and a documented disaster recovery plan.

CNS backs up data to tapes on a daily, weekly, and monthly basis. Tapes are rotated offsite weekly.

CNS has contracted with SunGard to maintain a disaster recovery site at its Reston, VA facility, and with the Department of Veterans Affairs to maintain workspace in Washington, DC should CNS facilities become unavailable.

CNS tested the Disaster Recovery Plan in August 2001.

Weaknesses: The business continuity plan has not been tested since 1999. The business continuity plan is currently under revision and will be finalized based upon the results of the disaster recovery plan testing that has recently been conducted. Business continuity and disaster recovery plans have not been developed for Service Centers or State offices. (severity: medium)

During the review of the disaster recovery plan, it was noted that the address of the off-site tape storage location was not listed. This information should be included in the disaster recovery plan. (severity: low)

5. Hardware and System Software Maintenance

Level 1	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
Yes	**Yes**	**Yes**	**Yes**	**No**

Strengths: Access to system software is restricted to a limited number of personnel, corresponding to job responsibilities. New system software versions or products and modifications to existing system software receive proper authorization and are supported by a change request document.

Weaknesses: Hardware and system software maintenance controls are not fully integrated into the Corporation's overall life cycle planning. The Corporation's System Development Life Cycle methodology is not applied to the network. (severity: low)

6. Data Integrity

Level 1	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
Yes	**Yes**	**Yes**	**Yes**	**Yes***

* some weaknesses observed

Strengths: CNS has an agency-wide policy on Safeguarding Sensitive Information and Documents that provides users with guidelines for storage, disposal and handling of sensitive information and documents. In addition, it has application specific policies, procedures and controls in place. It also has general personnel security, network access and facility access controls in place that in combination protect data integrity.

Weaknesses: None observed for systems on the CNS LAN. Issues with WBRS were noted in the FY 2000 financial statement audit. (severity: low)

7. DOCUMENTATION

Level 1	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
Yes	**Yes***	**No**	**No**	**No**

* some weaknesses observed

Strengths: CNS management states that because it is a relatively small agency, it is able to do much through the direct involvement of its IT staff and top management, and through frequent conversations with and among them; and therefore, there is much less of a need for documentation than in a larger agency.

Weaknesses: Because of its size and limited resources, CNS documents its processes when it is required by external authority, but usually favors informality. This relative lack of documentation creates a situation in which it is difficult for a manager, auditor or other person who has not been directly involved, to ascertain whether required processes are being done, informally, or not at all. (severity: low)

8. SECURITY AWARENESS, TRAINING AND EDUCATION

Level 1	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
Yes	**Yes**	**Yes**	**Yes**	**Yes**

Strengths: An ongoing, agency-wide security awareness program has been implemented. It includes first-time training for all new employees, contractors, and users, and periodic refresher training thereafter. Technical staff receive annual security training according to job responsibilities and needs. Employees see and agree to the rules of behavior during their mandatory annual security awareness training. A daily security reminder is automatically displayed to employees during their login process.

Weaknesses: None observed.

9. INCIDENT RESPONSE CAPABILITY

Level 1	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
Yes*	**Yes***	**Yes***	**Yes***	**No**

* some weaknesses observed

Strengths: CNS has documented Incident Response Guidelines that contain internal procedures to be followed if an incident is detected.

Weaknesses: CNS's Incident Response Guidelines do not specify under what circumstances external federal authorities will be notified, nor under what circumstances the CNS Office of Inspector General will be notified, as required by GISRA. They also do not call for notification to owners of interconnected systems. The procedure for contacting other parties, the points of contact, and the nature of the information to be provided to them is not described. The CIO acknowledges the requirement to update their reporting guidelines to comply with GISRA and is in the process of completing that task. In the interim, the CIO has indicated they will report security incidents to the OIG and to appropriate external authorities. (severity: medium)

C. TECHNICAL CONTROLS

1. IDENTIFICATION AND AUTHENTICATION

Level 1	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
Yes	**Yes**	**Yes***	**Yes**	**Yes**

* some weaknesses observed

Strengths: Access to CNS systems is granted on a need to know basis. Password policy and procedures are clearly documented and provided to all users. 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. Emergency and temporary access is not authorized until the standard access request procedures are followed. CNS authentication policies and procedures are consistent across all systems on the CNS LAN.

Weaknesses: CNS management is aware that some CNS users have weak passwords, and makes periodic efforts to educate users. Automated enforcement of strong passwords has not been implemented. Additional authentication methods are not used. Analysis of the WBRS been implemented. Additional authentication methods are not used. Analysis of the WBRS resulted in recommendations to improve access and password controls as well as verification of data inputs to the system. (severity: medium)

2. Logical Access Controls

Level 1	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
Yes	**Yes**	**Yes**	**Yes**	**Yes**

Strengths: CNS has documented policies and procedures that require access to CNS systems to be granted only on a need to know basis. At an application system level, users are required to have management approval of their request for system access. CNS access control policies and procedures are consistent across all systems on the CNS LAN.

Weaknesses: None observed for systems on the CNS LAN. During the OIG's audit of the Corporation's Financial Statement for Fiscal Year 2000[1], analysis of the WBRS identified weaknesses in access and password controls and in the verification of data inputs to the system. The report noted that WBRS password entry attempts are not limited to three attempts. Multiple failed attempts do not trigger a freezing of the account to defend the system against unauthorized access. There is no enforcement of the suggestion that passwords should be at least six characters long. The WBRS does not automatically log off after a period of thirty minutes of inactivity. Additionally, the report recommended routine review of WBRS error listings by an individual other than the person inputting data into the system and spot checks of underlying support for the data submitted via WBRS on a periodic basis. (severity: medium)

3. Audit Trails

Level 1	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
Yes	**Yes**	**Yes**	**Yes***	**No**

* some weaknesses observed

Strengths: The Network Computer Security Plan provides agency-wide, but specific guidance on the review of a variety of audit logs that are generated by the major CNS application systems, servers and network devices.

[1] OIG Audit Report Number 01-01, *Audit of the Corporation for National and Community Service's Fiscal Year 2000 Financial Statements*, and OIG Audit Report Number 01-02, *Recommended Improvements to the Corporation's Internal Controls Fiscal Year 2000 – Management Letter.*

Weaknesses: There is only verbal confirmation that the audit logs are regularly reviewed or otherwise analyzed. (severity: low) Audit trail controls are not fully integrated into the Corporation's overall life cycle planning. (severity: low).

APPENDIX B

OFFICE OF INSPECTOR GENERAL
CORPORATION FOR NATIONAL AND COMMUNITY SERVICE

LOCAL AND WIDE AREA NETWORKS
GISRA ASSESSMENT SUMMARY

BACKGROUND

The Corporation for National Service (CNS) Network consists of a local area network (LAN) in the headquarters office, with high speed Frame Relay network provided by MCI for remote Regional Service Centers, State Offices, National Civilian Community Corps (NCCC) campuses, and two remote processing sites. Web servers reside on the public side of the Corporation Network outside the headquarters firewall, and are provided by UUNET. 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.

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

ASSESSMENT OVERVIEW

The CNS Corporation Network is generally well-protected through a combination of sound security practices and continuing management attention.

Security policies relating to the Corporation Network are for the most part comprehensive and well documented, but some have not yet been updated to reflect GISRA requirements. These include the requirement for annual GISRA assessments; required reporting, when security incidents occur, to the Inspector General and external authorities, such as FEDCIRC; and integration of information security into the agency's strategic IT plan and overall agency resource prioritization processes.

Information security plans are in place, but are almost totally operational in nature. More strategic, forward looking elements should be incorporated in them that address such topics as the Corporation's plans for compliance with the Government Paperwork Elimination Act (GPEA) and GISRA, including the resources that will be required. Business Continuity Plans are not current and do not include CNS entities outside the Washington headquarters. They should be updated.

Procedures implementing network security policies are not as well documented as are the policies, but are generally effective. Areas that need strengthening include procedures for conducting risk assessments that incorporate business impact analysis and procedures for applying a System Development Life Cycle methodology to the network;

Security controls for the Corporation Network are generally effective. One area that needs improvement is the documentation of the results and review of audit logs and other security measures to assure actual performance of reviews. Another area is authentication. CNS management acknowledges that some CNS users have weak passwords, and makes periodic efforts to educate users. Automated enforcement of strong passwords has not been implemented, nor have additional methods of authentication been used.

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 following table summarizes the results of the assessment that was done based on the above standards and criteria. The remainder of this report summarizes the key strengths and weaknesses for each of the major control objectives. Each weakness is classified into a high, medium and low severity rating. Special weight was given to those areas that are directly addressed by the GISRA legislation.

One aspect of the ratings deserves mention. The criteria for meeting the Level 5 requirements of the Framework is integration of information security plans into the agency's strategic plans, and integration of the operational and technical controls into a life cycle methodology. Lack of these two elements causes all Level 5 ratings for the network to be negative. But, this should not overshadow the fact that CNS's information security practices are generally effective.

ASSESSMENT RATINGS SUMMARY

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

* some weaknesses observed

A. MANAGEMENT CONTROLS

1. RISK MANAGEMENT

Level 1	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
Yes	**No**	**Yes***	**Yes***	**No**

* some weaknesses observed

Strengths: CNS policy requires that network risk assessments be performed in conjunction with Corporation Network re-accreditations at least every three years. The current re-accreditation of the network was completed in February 2001, and is limited to a one year period. A risk analysis was completed as part of the re-accreditation process.

Weaknesses: Although risk assessments are periodically done in conjunction with re-accreditation, CNS does not have documented procedures for how to do the risk assessments. CNS contracts with a commercial vendor to perform this analysis and relies on the contractor's methodology and expertise. The risk analysis that was completed for the network this year found the risks overall to be low, but did not include a business impact analysis, nor an analysis at the network component level. Network resources are not classified according to their sensitivity or criticality. OIT has done informal assessments of risk at the network component level, and has in place active redundancy, backup equipment, and spare parts for critical elements of the Corporate Network. (severity: low)

A business impact analysis document does not exist, but business impacts were considered as the Disaster Recovery Plan (DRP) was being written. Impacts noted in the DRP are expressed as high, medium and low, and are not expressed in terms of functional impacts. (severity: medium)

Risk Management procedures and controls for the network are not fully integrated into the Corporation's overall life cycle planning. The Corporation's System Development Life Cycle methodology is not applied to the network. (severity: low)

2. REVIEW OF SECURITY CONTROLS

Level 1	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
Yes	**Yes**	**Yes***	**Yes**	**No**

* some weaknesses observed

Strengths: CNS policy requires that security control reviews be periodically conducted in accordance with OMB Circular A-130. A security controls review was completed in June 2001, as part of the re-accreditation process.

OIT regularly conducts its own tests of security controls, and periodically has penetration testing done by independent testers.

All users must log into the Windows NT network before logging into an application. Twelve State Offices, five Service Centers and all NCCC campuses are connected to the Corporation Network through a Frame Relay network provided by MCI. The other State Offices dial into a Cisco AS5300 configured as a Point-to-Point Protocol (PPP) server. Dial-in users must pass the AS5300's authentication routine of MS-CHAP which is provided by the Cisco Secure ACS software, and then must log into the NT network. Then the user may log into an application system under the control of an individual security profile.

Weaknesses: A GISRA assessment in accordance with the CIO Council's Federal Information Technology Security Assessment Framework was not done as required by OMB. In June 2001, a Security Controls Review was performed by a contractor as part of the network re-accreditation process, providing roughly equivalent information in many areas. (severity: low)

During August 2001, some vulnerabilities were discovered during KPMG's independent penetration testing done in conjunction with this GISRA assessment. CNS took some remedial actions. (severity: low)

Network security controls are not fully integrated into the Corporation's overall life cycle planning. The Corporation's System Development Life Cycle methodology is not applied to the network. (severity: low)

3. LIFE CYCLE

Level 1	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
Yes	**Yes***	**Yes***	**No**	**No**

* some weaknesses observed

Strengths: CNS has a System Development Life Cycle (SDLC) policy and methodology. On-going network security monitoring and pro-active measures, such as required security training, awareness building, an aggressive virus protection program, access controls, and remote site network management, are an indication of day to day management attention to security.

Weaknesses: CNS has a System Development Life Cycle (SDLC) policy and methodology, but it has not been formally applied to the Corporation Network. Management stated that the CNS SDLC is applied informally in their normal planning, acquisition, testing and implementation processes for new network equipment and systems. (severity: low)

4. AUTHORIZE PROCESSING (CERTIFICATION AND ACCREDITATION)

Level 1	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
Yes	**Yes**	**Yes**	**Yes**	**No**

Strengths: CNS policy requires re-accreditation of the Corporation's network every three years, in accordance with OMB Circular A-130. Re-accreditation of the network was completed in June 2001, for a one year period.

Weaknesses: Processing authorization is not fully integrated into the Corporation's overall life cycle planning. The Corporation's System Development Life Cycle methodology is not applied to the network. (severity: low)

5. SYSTEM SECURITY PLAN

Level 1	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
Yes	**Yes**	**Yes**	**Yes**	**No**

Strengths: CNS policy requires that each critical system have a system security plan. CNS has such a plan for the CNS network. The plan was updated as of June 2001, as part of the re-accreditation process.

Weaknesses: The Network Computer Security Plan is not fully integrated into the Corporation's overall life cycle planning. The Corporation's System Development Life Cycle methodology is not applied to the network. (severity: low)

A summary of the Security Plan is not included in the CNS Strategic IT Plan as required by GISRA. (severity: low)

B. OPERATIONAL CONTROLS

1. PERSONNEL SECURITY

Level 1	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
Yes*	**Yes***	**Yes***	**Yes**	**No**

* some weaknesses observed

Strengths: Job descriptions within OIT reflect assigned responsibilities, include requirements for technical knowledge, skills and abilities, and can be used for performance evaluations.

No one is authorized to bypass controls, or get access prior to the completion of the new employee computer security training and supervisory authorization processes.

Weaknesses: Separation of duties is not explicitly mentioned in the Corporation Computer and Network Policy. A "least privilege" access policy is implemented through job functions, roles, and need-to-know policies. Termination procedures are not formally specified for friendly vs. unfriendly terminations, but OIT is sensitive to potential threats, and takes action based on specific situations. (severity: low)

2. PHYSICAL AND ENVIRONMENT PROTECTION

Level 1	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
Yes	**Yes**	**Yes***	**Yes**	**No**

* some weaknesses observed

Strengths: The computer room at CNS headquarters that houses most of the network and server components that comprise the CNS network is a restricted access facility. All access is logged.

The computer room has an uninterruptible power supply that protects against power fluctuations and outages.

Access to the Corporation's offices is controlled by electronic access keys. Receptionists control access for those without access keys.

Weaknesses: OIG has previously reported weak accountability for the electronic access keys and the master keys that permit access to every floor. (severity: medium) Reception personnel do not consistently challenge visitors. (severity: low) A documented physical and environmental risk assessment to determine the adequacy of the physical controls has not been done. (severity: low)

Physical and environmental protection is not fully integrated into the Corporation's overall life cycle planning. The Corporation's System Development Life Cycle methodology is not applied to the network. (severity: low)

3. PRODUCTION INPUT/OUTPUT CONTROLS

Level 1	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
Yes	**Yes***	**Yes**	**Yes**	**No**

* some weaknesses observed

Strengths: Formal production input and output controls are in place for remote operations. A help desk at CNS headquarters provides first level support for questions and technical problems locally and nationally.

Weaknesses: Informal production input and output controls are in place in the CNS headquarters. (severity: low)

Production input and output controls are not fully integrated into the Corporation's overall life cycle planning. The Corporation's System Development Life Cycle methodology is not applied to the network. (severity: low)

4. CONTINGENCY PLANNING

Level 1	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
Yes	**Yes***	**Yes**	**Yes***	**No**

* some weaknesses observed

Strengths: A Corporate headquarters Disaster Recovery Plan (DRP) and Business Continuity/ Contingency Plan (BCCP) are in place. A draft DRP has been prepared by DOI-NBC for the Momentum system that includes telecommunications links. CNS tested the Disaster Recovery Plan in August 2001.

An update of the disaster recovery document is pending, and will be completed now that the disaster recovery test has been done. The Corporation has contracted for 100 seats at SunGard.

Weaknesses: The BCCP has not been tested. The Service Centers and State Offices depend upon headquarters OIT to restore their IT environment. They do not have documented business recovery plans or capabilities for recovery of business functions. The file servers at Service Centers are backed up to tape weekly on a four-week rotation. Tapes are kept in a safe located in a room adjacent to the server room. A tape is sent quarterly to headquarters for permanent archival. (severity: medium)

Contingency planning is not fully integrated into the Corporation's overall life cycle planning. The Corporation's System Development Life Cycle methodology is not applied to the network. (severity: low)

5. Hardware and System Software Maintenance

Level 1	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
Yes	**Yes**	**Yes**	**Yes**	**No**

Strengths: Access to system software is restricted to a limited number of personnel, corresponding to job responsibilities. New system software versions or products and modifications to existing system software receive proper authorization and are supported by a change request document.

Weaknesses: Hardware and system software maintenance controls are not fully integrated into the Corporation's overall life cycle planning. The Corporation's System Development Life Cycle methodology is not applied to the network. (severity: low)

6. Data Integrity

Level 1	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
Yes	**Yes**	**Yes**	**Yes**	**No**

Strengths: Various general controls are in place to protect data integrity. Inappropriate or unusual activity is investigated and appropriate actions taken. Technical management monitors the use of privileged system software and utilities. Procedures are in place to determine compliance with password policies. Intrusion detection tools are installed on the system. Internal and external penetration testing is performed as needed.

OIT maintains close ties with CERT, FedCIRC, SANS for virus alerts, keeps current with Cisco maintenance, and keeps current with virus detection updates from Macafee.

Weaknesses: Data integrity controls are not fully integrated into the Corporation's overall life cycle planning. The Corporation's System Development Life Cycle methodology is not applied to the network. (severity: low)

7. DOCUMENTATION

Level 1	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
Yes	**Yes**	**Yes**	**Yes**	**No**

Strengths: Network security policies and procedures are documented and current. The security plan establishes and documents the security controls.

Network diagrams document the network topology. Configuration parameters for routers and switches is documented.

Weaknesses: Documentation controls are not fully integrated into the Corporation's overall life cycle planning. The Corporation's System Development Life Cycle methodology is not applied to the network. (severity: low)

8. SECURITY AWARENESS, TRAINING AND EDUCATION

Level 1	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
Yes	**Yes**	**Yes**	**Yes**	**No**

Strengths: 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. Technical staff receive annual security training according to job responsibilities and needs. Employees see and agree to the rules of behavior during their mandatory annual security awareness training. A daily security reminder is automatically displayed to employees during their login process.

Weaknesses: Security Awareness, Training and Education controls are not fully integrated into the Corporation's overall life cycle planning. The Corporation's System Development Life Cycle methodology is not applied to the network. (severity: low)

9. INCIDENT RESPONSE CAPABILITY

Level 1	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
Yes*	**Yes***	**Yes***	**Yes***	**No**

* some weaknesses observed

Strengths: The current Incident Response Guidelines document is 27 pages long and highly technical. A new version of the guidelines is being written to make them easier for users to understand and follow.

Inappropriate or unusual activity is investigated and appropriate actions taken. Intrusion detection tools are installed on the system. Incident response policies and procedures are documented, implemented and updated as needed.

Weaknesses: CNS's Incident Response Guidelines do not address the conditions or procedures for involving the CNS Inspector General (IG) or external federal authorities, as required by GISRA. However, one incident was recently reported to both the OIG and FEDCIRC. Reporting procedures should be developed that describe under what conditions an incident should be reported to the IG or to authorities outside of the CNS such FEDCIRC or the FBI. The reporting procedures should describe to whom the incident is to be reported and the information to be provided in the report. (severity: medium)

Incident Response controls are not fully integrated into the Corporation's overall life cycle planning. The Corporation's System Development Life Cycle methodology is not applied to the network. (severity: low)

C. TECHNICAL CONTROLS

1. IDENTIFICATION AND AUTHENTICATION

Level 1	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
Yes	**Yes**	**Yes***	**Yes**	**No**

* some weaknesses observed

Strengths: Password policy and procedures are clearly documented and provided to all users. 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. Emergency and temporary access is not authorized until the standard access request procedures are followed.

Weaknesses: CNS management is aware that some CNS users have weak passwords, and makes periodic efforts to educate users. Automated enforcement of strong passwords has not been implemented. (severity: medium)

Identification and authentication controls are not fully integrated into the Corporation's overall life cycle planning. The Corporation's System Development Life Cycle methodology is not applied to the network. (severity: low)

2. LOGICAL ACCESS CONTROLS

Level 1	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
Yes	**Yes**	**Yes**	**Yes**	**No**

Strengths: Logical access controls are in place for the local and remote network.

In addition to controlling access to the network by user, CNS controls network access by port based on the MAC address of the PC or server.

Weaknesses: Logical access controls are not fully integrated into the Corporation's overall life cycle planning. The Corporation's System Development Life Cycle methodology is not applied to the network. (severity: low)

3. AUDIT TRAILS

Level 1	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
Yes	**Yes**	**Yes**	**Yes***	**No**

* some weaknesses observed

Strengths: 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.

Audit trails are produced by network system software, logging administrative and technical support activities performed by users.

Weaknesses: There is only verbal affirmation from management that the audit logs are regularly reviewed or otherwise analyzed. (severity: low)

Audit trail controls are not fully integrated into the Corporation's overall life cycle planning. The Corporation's System Development Life Cycle methodology is not applied to the network. (severity: low)

APPENDIX C

Office of Inspector General
Corporation for National and Community Service

Momentum
GISRA Assessment Summary

Background

Momentum is the financial management system for the Corporation for National Service (CNS). The Momentum application 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. Momentum is accessed through the CNS LAN by up to 150 users nationwide.

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 Memorandum of Agreement with the 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. Information in the system may be sensitive and is covered under the Privacy Protection Act. The Momentum system also transmits sensitive but unclassified data.

The "senior program official" in CNS responsible for Momentum, in accordance with GISRA, is Gerry Yetter, Director of Accounting.

Assessment Overview

Security policies relating to Momentum are generally comprehensive and well documented. However, policies should be updated to be in accordance with GISRA, and to specifically address the role of the senior program official responsible for Momentum in the assessment of risks, potential business impacts and degree of mitigation achieved through security controls.

Procedures implementing policies are not as well documented as the policies, but for the most part are effective. However, the recently conducted Momentum risk assessment did not specifically consider the business impact that would result, if Momentum became unavailable. This gap may result from the absence of CNS specific procedures for conducting risk assessments, and in this case relied on the judgment of the firm with whom they contracted for the re-accreditation assessments.

Momentum has three external interfaces: to the USDA National Finance Center, to the SPAN/TRUST interface and to the Department of Health and Human Services. Written authorization and a clear delineation of responsibilities for information security is not established for these external interfaces.

CNS policy requires re-accreditation of systems every three years, and re-accreditation includes a review of system controls. There is no policy for more frequent, on-going security controls review of Momentum. The re-accreditation done in 2001 was only for a one year period. CNS plans to repeat the process again during 2002.

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 following table summarizes the results of the assessment that was done based on the above standards and criteria. The remainder of this report summarizes the key strengths and weaknesses for each of the major control objectives. Each weakness is classified into a high, medium and low severity rating. Special weight was given to those areas that are directly addressed by the GISRA legislation.

ASSESSMENT RATINGS SUMMARY

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

* some weaknesses observed

A. MANAGEMENT CONTROLS

1. Risk Management

Level 1	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
Yes	**No**	**Yes***	**Yes**	**No**

* some weaknesses observed

Strengths: Risk assessments have been conducted for Momentum as part of the recent re-accreditation of the system, and in accordance with the CNS Computer Security policy.

Weaknesses: There are no documented agency-wide procedures specifying how risk assessments should be done, and, no documented procedures for evaluating business risk. In the most recent risk analysis Momentum outage impacts are only expressed as high, medium, and low. There has been no evaluation of the business impact that would result if Momentum functionality is lost. (severity: medium)

In accordance with GISRA requirements, CNS has recently instituted a procedure to have the appropriate senior program official formally accept responsibility for the levels of risk and mitigation within the systems that support mission critical programs. This has been done for Momentum. Policies, procedures, position descriptions, and other related documents should be updated to incorporate the GISRA requirements. (severity: low)

CNS policies require risk assessments to be performed at least every three years or as changes are implemented in the application system. GISRA requires a review annually, as opposed to every three years, as was previously required. Beginning in 2001, CNS is transitioning to annual assessments. (severity: low)

2. Review of Security Controls

Level 1	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
Yes	**Yes**	**Yes**	**Yes***	**Yes***

* some weaknesses observed

Strengths: Security controls for CNS's mission critical systems have been reviewed every three years in accordance with OMB A-130 re-accreditation requirements. A re-accreditation security review was done for Momentum in 2001.

Weaknesses: CNS's Network and Computer Security policy states that "The Corporation conducts an independent audit or review on all major application or general support systems every three years to verify the levels of protection are adequate and appropriate." CNS Network Computer Security Plan does not state the frequency of security controls reviews. GISRA requires a review annually, as opposed to every three years, as was previously required. A GISRA assessment, in accordance with OMB Memorandum M-01-08, using the CIO Council's Federal Information Technology Security Assessment Framework was not done. (severity: medium)

3. LIFE CYCLE

Level 1	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
Yes	**Yes**	**Yes***	**No**	**No**

* some weaknesses observed

Strengths: CNS has a systems development life cycle policy and methodology, and maintains documentation related to the Momentum application. A systems security plan for Momentum was developed during the accreditation process. CNS's Momentum application is in the operational phase of the system development life cycle. Operational security responsibilities for the Momentum system are divided between CNS staff and the National Business Center (NBC) staff. The application software was developed by AMS. NBC maintains a contract with AMS for system maintenance, and itself provides software configuration tracking of changes and enhancements per its Memorandum of Agreement with CNS.

Weaknesses: There is very little documentation to substantiate that a System Development Life Cycle (SDLC) process continues to be followed for Momentum.

4. AUTHORIZE PROCESSING (CERTIFICATION AND ACCREDITATION)

Level 1	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
Yes	**Yes**	**Yes***	**Yes**	**Yes***

* some weaknesses observed

Strengths: CNS has in place a computer security policy and plan that require applications to be re-accredited every 3 years. CNS's mission critical application systems, including Momentum, were officially re-accredited in June 2001. During this process a security evaluation, risk assessment and penetration testing were completed. Accreditation reports are developed and maintained as required.

Weaknesses: Momentum has three external interfaces: to the USDA National Finance Center, SPAN/Trust and the Department of Health and Human Services. Written authorization and a clear delineation of responsibilities for information security do not exist for these external interfaces. (severity: medium)

5. SYSTEM SECURITY PLAN

Level 1	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
Yes	**Yes**	**Yes**	**Yes**	**No**

Strengths: CNS maintains a system security plan for the Momentum application, in accordance with the CNS Computer Security Policy. The security plan was developed in accordance with NIST 800-18 guidance.

Weaknesses: A summary of Security Plans is not incorporated in the Corporation's Information Management Strategic Plan as required by GISRA. (severity: medium)

B. OPERATIONAL CONTROLS

1. PERSONNEL SECURITY

Level 1	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
Yes*	**Yes***	**Yes***	**Yes**	**Yes***

* some weaknesses observed

Strengths: Personnel security controls are in place for the Momentum system. Formal documented processes exist for requesting, issuing and establishing access and privileges within the Momentum application. CNS maintains computer security policy 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. User rights are reviewed quarterly for appropriateness.

Weaknesses: CNS does not perform extensive background checks on its employees. The Human Resources Office has not issued any written policies on employee screening, but reports that it does request a National Agency Check on employees serving in certain select positions after they are hired. This requirement does not apply to all personnel. Additionally, Corporation termination procedures are not formally documented. Procedures should be documented for both friendly and unfriendly terminations. (severity: medium) Rules of Behavior for Momentum have not been set forth and are still under development by the CNS Financial Systems Group. However, partially compensating controls exist. The Information Systems Request form requires users to acknowledge password security requirements, non-disclosure of government information, proper use of information, and legal responsibilities. (severity: low)

2. Physical and Environment Protection

Level 1	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
Yes	**Yes**	**Yes**	**Yes***	**Yes***

* some weaknesses observed

Strengths: Physical and environmental controls have been implemented for the Momentum application by the DOI National Business Center.

Weaknesses: The Service Level Agreement with the National Business Center does not address the facilities or environmental protection that is to be provided. GAO recently identified weak computer security controls at the National Business Center in GAO-01-615, "Interior Information Security: Weak Controls Place Interior's Financial and Other Data at Risk", issued in July 2001. (severity: low)

3. Production Input/Output Controls

Level 1	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
Yes	**Yes**	**Yes**	**Yes**	**Yes**

Strengths: User manuals are available for reference. The Momentum application has built in edit checks to ensure that data entered is within a valid character set. Reports generated from the Momentum system by CNS employees have a sensitivity designation. CNS management has stated that 1) the Financial Services group of CNS periodically performs reviews of transactions for budgeting purposes to investigate anomalies; 2) on a monthly basis a review of users requesting transactions is performed to ensure that appropriate personnel are making requests; and 3) a monthly review is also performed to ensure that users obligating funds are not making payments as well.

Weaknesses: Users who have a need to run a report in Momentum are all given the same user identification and password. This practice gives them the ability to run the Momentum reports needed, but it weakens accountability for who is accessing the data in the system. (severity: medium)

4. CONTINGENCY PLANNING

Level 1	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
Yes	**Yes**	**Yes**	**Yes***	**No**

* some weaknesses observed

Strengths: CNS maintains an agency wide Continuity of Operations Plan. The Department of the Interior National Business Center has continuity and disaster recovery procedures that would move the Momentum application to an alternate processing site in Denver, in the event of a disaster. CNS tested its disaster recovery plan in August 2001.

Weaknesses: The disaster recovery testing did not include business continuity plan testing. (severity: medium) The Department of the Interior National Business Center Momentum Disaster Recovery and Backup Plan is currently only in draft. (severity: medium)

5. HARDWARE AND SYSTEM SOFTWARE MAINTENANCE

Level 1	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
Yes	**Yes**	**Yes**	**Yes**	**Yes**

Strengths: Hardware and software maintenance and development controls are in place for the Momentum system. CNS follows a systems development lifecycle methodology. The application is currently in the operational phase and is operated by the Department of the Interior National Business Center (NBC). The Service Level Agreement with the NBC calls for the NBC to provide monitoring, maintenance and tracking of configuration changes for the hardware, system software, database software and telecommunications.

Weaknesses: None observed.

6. DATA INTEGRITY

Level 1	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
Yes	**Yes**	**Yes**	**Yes**	**Yes**

Strengths: Corporation management states that the Financial Services group periodically performs reviews of transactions for budgeting purposes to investigate anomalies. Specifically, on a monthly basis a review of users requesting transactions is performed to ensure that appropriate personnel are making requests. And also, a monthly review is performed to ensure that users obligating funds are not making payments as well. A user support help desk and training are available to assist users who experience problems with the Momentum application.

Weaknesses: None observed.

7. DOCUMENTATION

Level 1	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
Yes	**Yes**	**Yes**	**Yes**	**Yes**

Strengths: Documentation controls are in place for the Momentum system. AMS developed the Momentum application and provided user, administration and training manuals and guides to CNS. CNS management has stated that a Disaster Recovery Plan for the Momentum application hosted at the National Business Center is in draft.

Weaknesses: None observed.

8. SECURITY AWARENESS, TRAINING AND EDUCATION

Level 1	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
Yes	**Yes***	**Yes**	**Yes**	**Yes**

* some weaknesses observed

Strengths: Adequate security awareness and training programs are in place for the Momentum system. 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. Momentum specific training is provided on an as needed basis to Momentum users. An electronic version of the Momentum documentation is available on the Corporation's Intranet site.

Weaknesses: Rules of Behavior for the Momentum application are still under development by the CNS Financial Systems Group. (severity: low)

9. INCIDENT RESPONSE CAPABILITY

Level 1	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
Yes*	**Yes***	**Yes***	**Yes***	**No**

* some weaknesses observed

Strengths: CNS has documented Computer Incident Response Guidelines which specify internal reporting procedures for detected security incidents.

Weaknesses: CNS's Incident Response Guidelines do not address the conditions or procedures for involving the CNS Office of Inspector General (OIG) or external federal authorities, as required by GISRA. Reporting procedures should be developed that describe under what conditions an incident should be reported to the OIG or to authorities outside of the CNS such as FEDCIRC or the FBI. The reporting procedures should describe to whom the incident is to be reported and the information to be provided in the report. The CIO acknowledges the requirement to update the reporting guidelines to comply with GISRA and is in the process of completing that task. In the interim, the CIO has indicated they will report security incidents to the OIG and appropriate external authorities. (severity: medium) CNS should ensure that the National Business Center has procedures to notify the appropriate CNS authorities if an incident is detected relating to the Momentum application, and that such notification is included in the NBC Service Level Agreement. (severity: high)

C. TECHNICAL CONTROLS

1. IDENTIFICATION AND AUTHENTICATION

Level 1	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
Yes	**Yes**	**Yes***	**Yes**	**Yes**

* some weaknesses observed

Strengths: Identification and authentication controls are in place for the Momentum system. 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 assigned Momentum privileges are then required to provide a separate Momentum user name and password to login in to the application. Passwords are masked when the user logs in and users are required to change their password at a minimum every 90 days. CNS management has stated that lists of current users are generated quarterly (every 90 days) and are provided to management to review for appropriateness. Distribution of initial Momentum passwords and user account information is documented and the process is adequately controlled.

Weaknesses: CNS management acknowledges that some CNS users have weak passwords and makes periodic efforts to educate users. Automated enforcement of strong passwords has not been implemented. Additional authentication methods are not used. CNS has undocumented procedures for OIT to issue and reissue passwords. (severity: medium)

2. LOGICAL ACCESS CONTROLS

Level 1	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
Yes	**Yes**	**Yes**	**Yes**	**Yes**

Strengths: Logical access controls are in place for the Momentum system. CNS users are required to login to the CNS network before they are able to access the Momentum application. Users are required to use a separate login for the Momentum application. User accounts are reviewed quarterly to ensure that only authorized employees have accounts. Upon login to the CNS network a login banner is displayed. No separate login banner is displayed when users login to the Momentum application.

Weaknesses: None observed.

3. AUDIT TRAILS

Level 1	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
No	**Yes**	**Yes***	**Yes***	**No**

* some weaknesses observed

Strengths: A transaction journal logs every transaction that is processed. According to CNS management, periodic tests and reviews of the data are performed by the Financial Services group. Monthly tests are performed to verify that users requesting transactions are not obligating funds and that users obligating funds are not making payments. An additional monthly review is performed of the budgets for all transactions processed by Momentum. A quarterly review is performed to verify that access rights are appropriate. User manuals and training are provided that specify how to complete these functions within Momentum, and how to review the transaction logs.

Weaknesses: There is no policy that requires that the procedures and tests listed above be performed regularly. For instance, there is no policy that the "Security Access Violation Query" and "Override Error Log Query" reports be generated and reviewed regularly.

APPENDIX D

OFFICE OF INSPECTOR GENERAL
CORPORATION FOR NATIONAL AND COMMUNITY SERVICE

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

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 for National Service (CNS) program official responsible for SPAN is Charlene Dunn, Director of Trust Management.

ASSESSMENT OVERVIEW

Security policies relating to SPAN are generally comprehensive and well documented. However, in accordance with GISRA, policies should be updated to specifically address the role of the senior program official responsible for SPAN in the assessment of risks, potential business impacts and degree of mitigation achieved through security controls.

Procedures implementing policies are not as well documented as the policies, but for the most part are effective. For instance, the recently conducted SPAN risk assessment does not specifically consider the business impact that would result, if SPAN became unavailable. This gap may result from the absence of CNS specific procedures for conducting risk assessments. CNS contracts with a commercial vendor to perform this analysis and relies on its methodology and expertise.

General security controls are the same as for other systems on the CNS network. But SPAN specific security controls are not documented. For instance, there is no documentation of procedures for an on-going process of security controls review specifically for SPAN, and no documentation of procedures for handling and reviewing SPAN audit logs. Although CNS management has stated that the System Development Life Cycle methodology was followed during the recent integration of VMS into SPAN, there is little supporting SDLC documentation for SPAN.

As with other systems on the CNS network, CNS management acknowledges that some CNS users have weak passwords and makes periodic efforts to educate users. Automated enforcement of strong passwords has not been implemented. Additional authentication methods are not used.

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 following table summarizes the results of the assessment that was done based on the above standards and criteria. The remainder of this report summarizes the key strengths and weaknesses for each of the major control objectives. Each weakness is classified into a high, medium and low severity rating. Special weight was given to those areas that are directly addressed by the GISRA legislation.

ASSESSMENT RATINGS SUMMARY

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

* some weaknesses observed

A. MANAGEMENT CONTROLS

1. RISK MANAGEMENT

Level 1	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
Yes	**No**	**Yes***	**Yes**	**No**

* some weaknesses observed

Strengths: Risk Management policies for SPAN are documented and current. 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, and is effective for one year.

Weaknesses: There are no documented agency-wide procedures specifying how risk assessments should be done, and, no documented procedures for evaluating business risk. CNS contracts with a commercial vendor to perform this analysis and relies on its expertise. In the most recent risk analysis SPAN outage impacts are only expressed as high, medium, and low. There has been no evaluation of the business impact that results when SPAN functionality is lost. (severity: medium)

In accordance with GISRA requirements, CNS has recently instituted a procedure to have the appropriate senior program official formally accept responsibility for the levels of risk and mitigation within the systems that support mission critical programs. This has been done for SPAN. Policies, procedures, position descriptions, and other related documents should be updated to incorporate these GISRA requirements. (severity: low)

2. REVIEW OF SECURITY CONTROLS

Level 1	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
Yes	**Yes**	**Yes**	**Yes***	**Yes***

* some weaknesses observed

Strengths: CNS policy requires that the security controls for mission critical systems be reviewed every three years as part of the re-accreditation process. A recent review of SPAN security controls was performed. The report is included in the SPAN Accreditation document dated June 21, 2001, and is effective for one year.

Weaknesses: A GISRA assessment in accordance with the CIO Council's Federal Information Technology Security Assessment Framework was not done. The SPAN Security Controls Review Report included with the SPAN Accreditation Report does not indicate any controls testing that may have been conducted during the SPAN accreditation process. In addition, there is no evidence that during the recent integration of VMS into SPAN any new controls have been tested to ensure that the new controls meet security specifications. (severity: low)

No documentation has been identified that demonstrates that an on-going process is in place to evaluate the effectiveness of SPAN security controls, or to maintain adequate protections. (severity: low)

3. LIFE CYCLE

Level 1	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
Yes	**Yes**	**Yes***	**No**	**No**

* some weaknesses observed

Strengths: 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. SPAN is now in its operational phase.

Weaknesses: There is little documentation to substantiate that an SDLC process was followed during the recent integration of VMS into SPAN, and also, little documentation of a change control process used for applying vendor-provided maintenance updates to Oracle, the operating system software, and the security software. Lack of such documentation could hinder an investigation of the source of problems, if a security incident were to occur. (severity: low)

CNS uses Oracle Designer/2000 for application software development and maintenance. Oracle Designer/2000 contains built-in security functions for application-specific privileges and roles, provides quality control, and includes reporting capabilities for detailed system design documentation. This provides some compensating controls.

4. AUTHORIZE PROCESSING (CERTIFICATION AND ACCREDITATION)

Level 1	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
Yes	**Yes**	**Yes**	**Yes**	**Yes**

Strengths: In accordance with CNS policies, SPAN, was formally re-accredited in June 2001 for one year. During the re-accreditation process a security evaluation and risk assessment were completed, and a security plan developed.

Weaknesses: None observed.

5. SYSTEM SECURITY PLAN

Level 1	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
Yes	**Yes**	**Yes**	**Yes**	**No**

Strengths: CNS has developed and implemented a security plan for the SPAN application, in accordance with the CNS Computer Security Policy. The plan is included in the SPAN accreditation document dated June 21, 2001. The accreditation process included a review of procedures and controls.

Weaknesses: The SPAN Security Plan is not summarized in CNS's Information Management Strategic Plan, as required by GISRA. (severity: low)

There is no business case document that defines the resources required for the on-going security of the SPAN system. (severity: low)

B. OPERATIONAL CONTROLS

1. PERSONNEL SECURITY

Level 1	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
Yes*	**Yes***	**Yes***	**Yes**	**Yes***

* some weaknesses observed

Strengths: Personnel security controls are in place for the SPAN application system. Documented processes exist for requesting, issuing and establishing access rights and privileges within the SPAN application. CNS management states that established procedures and controls are not bypassed to allow emergency access. CNS maintains computer security policy based on the concept of least privilege, which requires that users only have access to that information which they require to complete their job function. CNS personnel security policies and procedures are consistent agency-wide.

Weaknesses: Policies and procedures address accountability, and need-to-know for access to information and processing, but do not explicitly address separation of duties. CNS does not perform extensive background checks on its employees. The Human Resources Office has not issued any written policies on employee screening, but reports that it does request a National Agency Check on employees serving in certain select positions after they are hired. This requirement does not apply to all personnel. Employee termination procedures are not documented. Termination procedures should be documented and include procedures for both friendly and unfriendly terminations. (severity: low)

2. PHYSICAL AND ENVIRONMENT PROTECTION

Level 1	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
Yes	**Yes***	**Yes***	**Yes***	**No**

* some weaknesses observed

Strengths: The computer room at CNS headquarters where SPAN operates is a restricted access facility. Access to the computer room is logged.

Access to general office areas are controlled by electronic access keys. Receptionists control access for those without access keys.

The computer room has an uninterruptible power supply that will allow time for an orderly shutdown of systems, if a power outage occurs.

Weaknesses: Physical controls are in place, but a physical and environmental risk assessment has not been done. Controls may not be aligned with actual threats and vulnerabilities. For instance, plumbing line locations are not documented, so computer equipment and business records may be vulnerable to water damage. (severity: low)

OIG has previously reported weak accountability for the electronic access keys and for the master keys that control access to every floor. There are no documented requirements or procedures for securing unused keys. (severity: medium) Reception personnel do not consistently challenge visitors. (severity: low)

3. PRODUCTION INPUT/OUTPUT CONTROLS

Level 1	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
Yes	**Yes***	**Yes***	**Yes**	**Yes***

* some weaknesses observed

Strengths: Separate test and development platforms and controls over migrating software into the production environment control unauthorized access to production systems.

There is no central operations staff for SPAN, except that a help desk at CNS headquarters provides first level support for questions and technical problems locally and nationally. SPAN users control the input and output processes.

Weaknesses: Production input and output controls are informal at CNS headquarters. (severity: low)

4. CONTINGENCY PLANNING

Level 1	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
Yes	**Yes**	**Yes**	**Yes***	**No**

* some weaknesses observed

Strengths: A Corporation headquarters Disaster Recovery Plan (DRP) and Business Continuity / Contingency Plan (BCCP) are in place.

Weaknesses: The headquarters DRP was tested in August 2001. The BCCP has not been tested. Distribution of the DRP and BCCP is not documented. Employee training in recovery roles and responsibilities is not documented. (severity: low)

The Service Center and State Office that were reviewed depend upon headquarters OIT to restore their IT environment. They do not have documented business recovery plans or capabilities for recovery of business functions. The file server at the Service Center is backed up to tape weekly on a four-week rotation. Tapes are kept in a safe located in a room adjacent to the server room. A tape is sent quarterly to headquarters for permanent archival. (severity: low)

5. HARDWARE AND SYSTEM SOFTWARE MAINTENANCE

Level 1	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
Yes	**Yes***	**Yes***	**Yes***	**No**

* some weaknesses observed

Strengths: Change control procedures are in place to ensure the integrity and stability of production hardware and software systems. Separate test and development platforms and controls over migrating software into the production environment prevent unauthorized access to production systems.

Access to system software is restricted to a limited number of personnel, corresponding to job responsibilities. New system software versions or products and modifications to existing system software receive proper authorization and are supported by a change request document.

Weaknesses: An informal impact analysis is conducted to determine the effect of proposed changes on existing security controls, including the required training needed to implement the control. (severity: low) There is no documentation showing that system components are tested and approved (operating system, utility, applications) prior to promotion to production. (severity: low) There is no documentation showing that there are detailed system specifications prepared and reviewed by management. (severity: low) There is no documentation showing the type of test data to be used, i.e., live or made up. (severity: low) There is no documentation showing that there are software distribution implementation orders including effective date provided to all locations. (severity: low) There is no documentation showing that the distribution and implementation of new or revised software is documented and reviewed. (severity: low) There is no documentation showing that emergency changes are documented and approved by management, either prior to the change or after the fact. (severity: low) There is no documentation showing that contingency plans and other associated documentation are updated to reflect system changes. (severity: low)

6. DATA INTEGRITY

Level 1	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
Yes	**Yes***	**Yes***	**Yes**	**Yes***

* some weaknesses observed

Strengths: Data integrity and validation controls are used to provide assurance that the information has not been altered and the system functions as intended.

SPAN data integrity is maintained through access control procedures. Users are restricted based on need-to-know, and the principle of "least privilege" as determined and authorized by the employee's supervisor. Corrections to invalid entries in the database cannot be made using the Oracle Forms interface. Corrections can only be made by a designated SPAN user who is given temporary SQL access, and only after justification for the action is provided and the change is approved by the Director of the National Service TRUST, the Deputy CIO, the DBA, and the Information Systems Security Officer.

Inappropriate or unusual activity on the SPAN system is investigated and appropriate actions taken.

Procedures are in place to determine compliance with password policies.

Penetration testing is performed on the SPAN system when changes are significant enough to warrant re-testing.

Weaknesses: There is no documentation concerning whether reconciliation routines are used for the SPAN application, i.e., checksums, hash totals, record counts. (severity: low)

There is no documentation showing that integrity verification programs are used by the SPAN application to look for evidence of data tampering, errors, and omissions. (severity: low)

WBRS provides data that feeds into SPAN. Because access to WBRS is controlled by many organizations, and is not under CNS direct control, there is a potential for the WBRS data to be corrupted. That could result in unreliable data being passed to SPAN. (severity: low)

There is no documentation showing that system performance monitoring is used to analyze system performance logs in real time to look for availability problems, including active attacks. (severity: low)

7. DOCUMENTATION

Level 1	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
Yes	**Yes***	**Yes**	**Yes**	**Yes***

* some weaknesses observed

Strengths: User documentation for the SPAN application is available on-line. Oracle system documentation is also maintained on-line. The Oracle Designer/2000 tool is used to document business requirements, visually model the database schema, produce the entity relationship diagram, and create the database schema. Designer/2000 is also used to document the internal processes and configuration of the SPAN application.

Weaknesses: The following types of documentation are lacking:

- written agreements regarding how data is shared between interconnected systems (severity: low);
- backup procedures specific to the SPAN application and system software (severity: low); and
- software and hardware testing procedures and results (severity: low).

8. SECURITY AWARENESS, TRAINING AND EDUCATION

Level 1	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
Yes	**Yes**	**Yes**	**Yes**	**Yes**

Strengths: All 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. SPAN-specific training is provided for users as needed, and a help desk provides additional support for questions and problems. The SPAN Operator's Guide also emphasizes the user's security responsibilities. Information technology and security personnel attend conferences and specialized training to further their knowledge of security.

Weaknesses: None observed.

9. INCIDENT RESPONSE CAPABILITY

Level 1	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
Yes*	**Yes***	**Yes***	**Yes***	**No**

* some weaknesses observed

Strengths: CNS has documented Computer Incident Response Guidelines which specify internal reporting procedures for detected security incidents.

CNS management states that alerts/advisories are routinely received from multiple external sources, and appropriate action taken.

Weaknesses: CNS's Incident Response Guidelines do not specify under what circumstances external federal authorities will be notified, nor under what circumstances the CNS Office of Inspector General will be notified, as required by GISRA. They also do not address notification to owners of interconnected systems. The procedure for contacting other parties, the points of contact, and the nature of the information to be provided to them is not described. The CIO acknowledges the requirement to update the reporting guidelines to comply with GISRA and is in the process of completing that task. In the interim, the CIO has indicated they will report security incidents to the OIG and appropriate external authorities. (severity: medium)

The following types of documentation are lacking:

- documentation showing that incidents are monitored and tracked until resolved (severity: low); and
- documentation showing that personnel are trained to recognize and handle incidents (severity: low).

C. TECHNICAL CONTROLS

1. IDENTIFICATION AND AUTHENTICATION

Level 1	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
Yes	**Yes**	**Yes***	**Yes**	**Yes**

* some weaknesses observed

Strengths: All CNS users are required to identify and authenticate themselves, by providing valid username and password at the network level. CNS users who have been assigned SPAN privileges are then required to provide a separate, unique SPAN user name and password to log into the application. Passwords are masked when the user logs in and users are required to change their password at a minimum every 90 days. Lists of current users are generated quarterly (every 90 days) and are provided to management to review for appropriateness. Accounts are disabled after five failed logon attempts. New SPAN accounts are locked if they are not used within 30 days. Existing accounts are locked if passwords are not changed after 90 days. Procedures are in place for handling lost and compromised passwords. All actions are logged and correlated with users by the system. CNS authentication procedures are consistent agency-wide.

Weaknesses: CNS management acknowledges that some CNS users have weak passwords and makes periodic efforts to educate users. Automated enforcement of strong passwords has not been implemented. Additional authentication methods are not used. (severity: medium)

2. LOGICAL ACCESS CONTROLS

Level 1	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
Yes	**Yes**	**Yes**	**Yes**	**Yes**

Strengths: CNS users are required to log into the CNS network before they are able to access the SPAN application. Once logged on, the user is restricted to functions and transactions based on job duties. Oracle is able to restrict access to authorized relations, tables, views, data elements, and operations. Users are prohibited access to the SQL prompt. Access control software prevents one individual from having the necessary authority or information access to allow fraudulent activity without collusion.

There is no direct dial-in to SPAN, and no public access. State offices dial into the Corporation Network and must be properly authenticated before gaining access to SPAN. SPAN resides inside the Corporation Network firewall and is protected by an intrusion detection system. It is CNS policy not to authorize emergency and temporary access until proper procedures are followed. CNS management states that the SPAN access control list is internally encrypted on the SPAN computer system.

CNS authentication procedures are consistent agency-wide.

Weaknesses: WBRS provides data that feeds into SPAN. Because access to WBRS is controlled by many organizations, and is not under CNS direct control, there is a potential for the WBRS data to be corrupted. That could result in unreliable data being passed to SPAN. (severity: low) The following types of documentation are lacking:

- documentation indicating that terminals automatically log off and screensavers lock the session after a period of inactivity (severity: low); and
- documentation indicating whether access is restricted to files at the record level or field (data element) level (severity: low).

3. AUDIT TRAILS

Level 1	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
Yes	**Yes***	**Yes***	**Yes***	**No**

* some weaknesses observed

Strengths: Audit trails provided by the network operating systems ensure accountability at the network level. SPAN audits all database activity, and the audit reports are reviewed daily. All SPAN activity is recorded in the audit log including date, time, user ID, and description of activity.

Weaknesses: The following types of documentation are lacking:

- documentation describing how often SPAN audit trails should be reviewed, and actual frequency of review (severity: low);
- documentation to indicate whether automated tools are used to review SPAN audit records in real time or near real time (severity: low);
- documentation to indicate whether there is separation of duties between security personnel who administer the access control function and those who administer the SPAN audit trail (severity: low); and
- documentation to indicate whether SPAN audit logs stored off-line are retained for a specified period of time, and if so, whether access to audit logs is strictly controlled (severity: low).

APPENDIX E

OFFICE OF INSPECTOR GENERAL
CORPORATION FOR NATIONAL AND COMMUNITY SERVICE

GISRA EXECUTIVE SUMMARY

A. GENERAL OVERVIEW

Question 1. Identify the agency's total security funding as found in the agency's FY01 budget request, FY01 budget enacted, and the FY02 budget request.

Response to Question 1: No OIG response to this question is required since OMB's guidance indicates it is directly solely to the Corporation for National Service.

Question 2. Identify the total number of programs included in the program reviews or independent evaluations.

Response to Question 2: Self-assessments were done by program managers and the CIO of application systems deemed mission critical. In response to GISRA requirements, the OIG during July through September 2001 contracted with KPMG to perform evaluations of agency-wide information security policies and procedures and also to conduct independent evaluations of three of the four Corporation systems (Momentum Financial Management System, Corporation Network, and the System for Programs, Agreements and National Service Participants (SPAN)). The OIG did not re-evaluate the Web Based Reporting System (WBRS) at this time since it was assessed in conjunction with the recent audit of the Corporation's Financial Statement for Fiscal Year 2000. That audit and the associated Management Letter included recommendations for improvements in access and password controls and verification of data inputs to the system. As part of the audit resolution process, the Corporation agreed to consider recommended changes to WBRS. OIG will again evaluate the effectiveness of WBRS controls as part of the audit of the Fiscal Year 2001 Financial Statement.

Question 3. Describe the methodology used in the program reviews and the methodology used in the independent evaluations.

Response to Question 3: OIG and KPMG used the CIO Council's Federal IT Security Assessment Framework methodology in conjunction with control criteria from the NIST draft Special Publication, "Self-Assessment Guide for Information Technology Systems." Control techniques were derived from the related NIST publications, especially NIST SP 800-18, "Generally Accepted Principles and Practices for Securing Information Technology Systems". The NIST SP 800-18 control techniques were augmented by FISCAM control techniques.

Question 4. Report any material weakness in policies, procedures, or practices as identified and required to be reported under existing law.

Response to Question 4: No material weaknesses were identified during the CIO assessments or IG evaluations.

B. SECURITY PROGRAM PERFORMANCE

Question 5. What performance measures are used by the agency to ensure that program officials have:

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. Include information on the actual performance for each of the four categories.

Response to Question 5: All of CNS's mission critical systems completed a formal re-accreditation process in 2001. The re-accreditation included:

1) a risk assessment and determination of the level of security appropriate to protecting the programs' operations and assets;
2) an up-to-date security plan;
3) a security controls review; and
3) independent tests and evaluations of the security controls and techniques.

CNS senior program managers reviewed the results of the re-accreditation process and signed an affidavit for each of the mission critical systems. The affidavit certifies that they understand the risks to the operations and assets under their control, and accept responsibility for the degree of security provided to protect such operations and assets.

Question 6. The specific measures of performance used by the agency to ensure that the agency CIO:

1) adequately maintains an agency-wide security program;
2) ensures the effective implementation of the program and evaluates the performance of major agency components; and
3) ensures the training of agency employees with significant security responsibilities. Include information on the actual performance for each of the three categories.

Response to Question 6:

1) The CIO contracted for independent evaluations of all mission critical systems and the corporate network in 2001. The results of the independent evaluations were reviewed and approved by senior program officials. In addition, the IG conducted a separate GISRA evaluation specifically of agency-wide information security policies and procedures.
2) The CIO contracted for independent evaluations of all mission critical systems and the corporate network in conjunction with system re-accreditations. The OIG performed separate independent reviews of mission critical systems, the network and agency-wide policies and procedures.
3) 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 2001, five IT security specialists have attended eight security training classes and conferences.

Questions 7. Describe how the agency ensures that employees are sufficiently trained in their security responsibilities. Identify the total number of agency employees and briefly describe what types of security training was available during the reporting period, the number of agency employees that received each type of training, and the total costs of providing such training.

Response to Question 7: An ongoing, agency-wide security awareness program has been implemented. It includes first-time training for all new employees, contractors, and users, and yearly refresher training thereafter. All Corporation employees and contractors are required to complete annual security awareness training. Training requires all CNS users to acknowledge rules and guidelines by which they must abide. A daily security reminder is automatically displayed to employees during their log in process. In addition, application system user guides emphasize the user's security responsibilities.

The number of CNS employees and contractors who received first time security training during 2001 is about 200. All CNS employees and contractors, totaling approximately 750 individuals, received refresher security training during the year. The total cost of providing such training was approximately $7,500 in contractor costs.

Question 8. Describe the agency's documented procedures for reporting security incidents and sharing information regarding common vulnerabilities. Include a description of procedures for external reporting to law enforcement authorities and to the General Services Administration's FEDCIRC. Include information on the actual performance and the number of incidents reported.

Response to Question 8: The following is quoted from the CNS "Computer Incident Response Guidelines".

> "If a computer security incident is detected, it must be reported immediately to the OIT (Office of Information Technology) Director and the ISSO (Information Systems Security Officer). In particular, each end user must know how to contact the Director of OIT and the ISSO.
>
> The Director of OIT has the responsibility to report incident information to upper management in a timely fashion. In addition, the ISSO must report to the Director of OIT promptly in the event of a serious breach of security. If there is evidence of criminal activity, it is the responsibility of the OIT Director and ISSO to notify the Corporation's OIG.
>
> CAUTION: No Corporation staff member, except the designated Corporation spokesperson (and FBI, if involved) has authority to discuss any security incident with any person, agency, or organization that is not in his or her chain of command."

In this calendar year, one incident has been reported to the Corporation's OIG and to FEDCIRC. The Corporation recognizes the need to revise its guidelines to comply with GISRA's new reporting requirements.

Question 9. Describe how the agency integrates security into its capital planning and investment control process. Were security requirements and costs reported on every FY02 capital asset plan (as well as exhibit 53) submitted by the agency to OMB? If no, why not?

Response to Question 9: CNS is a relatively small organization with a limited number of senior officials. According to Corporation management, the same senior officials comprise the Corporation's resource investment board and are involved in all day to day policy decisions. Consequently, many resource investment decisions are handled as day to day business, rather than being held for a formal board meeting.

Security requirements and costs were included, but not separately identified, in the FY02 capital asset plan. An estimate of security costs was provided in the Exhibit 53 for FY02 submitted to OMB.

Question 10. Describe the specific methodology (e.g., Project Matrix review) used by the agency to identify, prioritize, and protect critical assets within its enterprise architecture, including links with key external systems. Describe how the methodology has been implemented.

Response to Question 10: CNS has no national responsibilities for critical infrastructure protection. It has a relatively simple technical infrastructure for its internal operations. Most of the Corporation's servers and network components are centralized in one Washington, D.C. facility. That facility supports all of the Corporation's mission critical applications. It has external links to two systems whose operations are outsourced, a link to an alternate service provider for payroll, and a link to a backup and recovery site. Because of the high degree of centralization, and limited number of critical external links, there is only one security infrastructure that protects all critical assets.

Question 11. Describe the measures of performance used by the head of the agency to ensure that the agency's information security plan is practiced throughout the life cycle of each agency system. Include information on the actual performance.

Response to Question 11: The Corporation is currently developing only one new automated system, the Grants Management System (GMS). OIG has contracted with KPMG LLP to conduct a risk assessment of the GMS, including a review of development methods and the adequacy of internal controls for information security. This assessment is a prelude to OIG's certification of the GMS, as mandated by the Departments of Veterans Affairs and Housing and Urban Development, and Independent Agencies Appropriations Act for Fiscal Year 2001 (Public Law 106-377), once GMS achieves initial operational capability in approximately April 2002.

The Corporation's planning and periodic status reporting documents show that the SDLC methodology has been used and that consideration has been given to security controls in the SDLC phases that have been completed for GMS to date. Additionally, frequent reviews of the GMS development project are being done by senior management, including a personal review by the Corporation's Chief Operating Officer at the completion of each major SDLC phase.

Question 12. Describe how the agency has integrated its information technology security program with its critical infrastructure protection responsibilities, and other security programs (e.g., physical and operational).

Response to Question 12: CNS makes no distinction between the critical infrastructure protection and information technology security programs. They are managed as one and the same. There is no separate prioritization of needs or resources.

Question 13. Describe the specific methods (e.g., audits or inspections) used by the agency to ensure that contractor provided services (e.g., network or website operations) or services provided by another agency are adequately secure and meet the requirements of the Security Act, OMB policy and NIST guidance, national security policy, and agency policy.

Response to Question 13: CNS has two mission critical systems that are out-sourced, one to another government agency and one to a commercial firm. In 2001, the CIO contracted for security assessments of these systems as part of the re-accreditation process. External penetration testing was a part of those security system assessments. The OIG also did an independent evaluation of the system out-sourced to another government agency. The evaluation included both external and internal penetration testing. The testing results were generally favorable.