Federal Communications Commission
Office of Inspector General

FY 2002 Government Information Security Reform Act (GISRA) Independent Evaluation

September 16, 2002

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Background

The Government Information Security Reform Act ("GISRA" or "the Security Act") was signed into law as part of the Fiscal Year (FY) 2001 Defense Authorization Act (Public Law 106-398). The Security Act amended the Paper Reduction Act of 1995 by adding a new subchapter on information security. The Security Act, which became effective on November 30, 2000, applies to all Federal agencies.

A key provision of the Security Act requires that the agency Office of Inspector General (IG), or independent evaluators designated by the IG, perform an annual evaluation of the agency's information security program and practices. The Federal Communications Commission's ("the Commission" or "FCC") IG engaged KPMG, LLP to conduct the independent evaluation of the FCC's information security program and practices for FY 2002.

The purpose of the evaluation was to review the Commission's security program including, but not limited to, security policies, security architecture, business continuity, security capital planning, critical infrastructure, and security program planning and management.

Using the National Institute of Standards and Technology (NIST) "Self-Assessment Guide for Information Technology Systems (Self-Assessment Guide)" as a basis for our methodology, our objective was to evaluate the effectiveness of the Commission's information security program by assessing the risk for each component of the program. As applicable, additional guidance was received from the methodology provided in the Federal Information System Control Audit Manual (FISCAM), as well as other laws and directives related to management and protection of Federal information resources.

The Office of Management and Budget's (OMB) Memoranda M-01-08, entitled "Guidance on Implementing the Government Information Security Act" and M-02-09, entitled "Reporting Instructions for the Government Information Security Reform Act and Updated Guidance on Security Plans of Action" were followed to perform and report the results of the independent evaluation.

Evaluation Objective

Our objective was to evaluate the effectiveness of the Commission's information security program by assessing the risk for each component of the program. The evaluation encompassed a review of the Commission's security program including security policies, security architecture, business continuity, security capital planning, critical infrastructure, and security program planning and management.

The specific objectives of this review were as follows:

1. Obtain an understanding of the Commission's Information Technology (IT) infrastructure.

2. Obtain an understanding of the Commission's information security program and practices.

3. Use the GISRA security assessment (i.e. NIST Self-Assessment Guide and FISCAM) tools to evaluate the effectiveness of the Commission's information security program and assess risk for each component of the program. At a minimum, the assessment was required to include an identification and ranking of the critical IS threats to the FCC IT infrastructure on a risk vulnerability basis.

4. Prepare the annual submission in accordance with the OMB reporting requirements mandated under GISRA for FY 2002. In addition to preparing the annual submission, the contractor was required to provide a detailed report that (1) identifies and ranks the critical security risk factors and (2) contains observations and recommendations for improvements, if any.

5. Follow-up on the findings of the Fiscal Year 2001 GISRA review that are documented in OIG report number, 01-AUD-11-43 and entitled Report on Government Information Security Reform Act Evaluation - Findings and Recommendations, issued November 29, 2001.

Evaluation Scope

The scope of our independent evaluation included the security infrastructure managed by the Office of Managing Director's Information Technology Center (ITC) and the Auctions Automation Branch of the Commission's Wireless Telecommunications Bureau (WTB). The Security Act also requires that agencies select an appropriate subset of business applications for review. Our audit of the Automated Auction System, follow-up audit of computer control conditions at the FCC's Consumer Center, and audit of Auctions physical security controls satisfy this requirement. The conclusions of these audits are being included with the results of our independent evaluation of the Commission's information security program and practices.

The evaluation encompassed a review of the Commission's security program including, but not limited to, security policies, security architecture, business continuity, security capital planning, critical infrastructure, and security program planning and management. During our evaluation we reviewed documentation provided by the Commission, reviewed previously performed special reviews and audits, conducted interviews of Agency staff, and performed other activities of inquiry and observation.

Our procedures were designed to comply with applicable auditing standards and guidelines, specifically the Generally Accepted Government Auditing Standards (GAGAS).

The evaluation methodology used was the National Institute of Standards and Technology (NIST) "Self-Assessment Guide for Information Technology Systems (Self-Assessment Guide)". As applicable, the methodology prescribed by the Federal Information Security Control Audit Manual (FISCAM) was used to assess management, operational, and technical controls during our risk assessment, as well as the following laws and directives related to management and protection of Federal information resources:

- Presidential Decision Directive (PDD) 63, entitled "Critical Infrastructure Protection."
- PDD-67, entitled "Continuity of Operations Planning (COOP)".
- OMB Circular A-130, entitled "Management of Federal Information Resources," as revised on November 30, 2000.
- OMB M-01-08, entitled "Guidance on Implementing the Government Information Security Reform Act," dated January 16, 2001.
- OMB M-97-16, entitled "Information Technology Architectures."
- OMB M-97-02, entitled "Funding Information Systems Investments."
- The Computer Security Act of 1987 (PL 100-235).
- OMB M-01-24, entitled "Reporting on the Government Information Security Reform Act," dated June 22, 2001
- FCC Instruction 1479.2, "Computer Security Program Directive."

Our observations have been organized according to the NIST control areas of management controls, operational controls, and technical controls. The control areas are defined below and the specific control techniques addressed by each are outlined.

Management Controls – Management controls focus on the management of the IT security system and the management of risk for a system. They are techniques and concerns that are normally addressed by management. The specific management control objectives addressed were:

- Risk Management
- Review of Security Controls
- Life Cycle
- Authorize Processing (Certification and Accreditation)
- System Security Plan

Operational Controls – Operational controls address security methods focusing on mechanisms primarily implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise and often

rely upon management activities as well as technical controls. The specific operational control objectives addressed are:

- Personnel Security
- Physical and Environmental Protection
- Production, Input/Output Controls
- Contingency Planning
- Hardware and System Software Maintenance
- Data Integrity
- Documentation
- Security Awareness, Training and Education
- Incident Response Capability

Technical Controls - Technical controls focus on security controls that the computer system executes. The controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. The specific technical operational control objectives addressed are:

- Identification and Authentication
- Audit Trails
- Logical Access Controls

Results of Fiscal Year 2002 Independent Evaluation

We have concluded that the Federal Communications Commission is dedicated to implementing and maintaining effective security control measures throughout the agency. Our independent evaluation for the current fiscal year and audit/follow-up audits of the Automated Auction System, Consumer Center, and Auctions Physical Security yielded several positive observations relative to the Commission's information security program and practices.

During the prior year's independent evaluation, security deficiencies were reported and recommendations for improvement made to the agency. The Commission developed and has reported on a quarterly basis its plan of actions and milestones (POA&M) for each finding, as required by OMB M-01-24, "Reporting Instructions for the Government Information Security Reform Act". As indicated in the POA&Ms issued to OMB, FCC management is effectively monitoring and tracking the progress of the corrective actions planned for each of the prior year's findings. We identified that several of the FY 2001 findings have been corrected and that corrective action has been defined and/or enacted for all others.

The FCC's IT Strategic Plan was published in June of 2002. The plan outlines the near and long-term directions for the agency's IT architecture and program. It also sets forth goals which reflect the core mission and values of the IT program as well as the agency's

core strategy goals of Broadband, Spectrum, Media, Homeland Security, Competition, and Modernizing the FCC. The agency is also in the process of developing a Computer Security Strategic Plan which will address management, operational, and technical controls, physical protection of information resources, and future computer security needs of the Commission.

During the reporting year, ITC, in a joint effort with system owners, completed security plans for sixteen (16) of its seventeen (17) major applications and general support systems, including the Automated Auction System, and the Auctions Network general support system. A security plan was also developed for the FCC's Consumer Center. Our review of the plans indicates that they incorporate elements recommended by OMB Circular A-130. Each security plan also includes newly developed Rules of Behavior for application users to execute. Additionally, Security Tests and Evaluations (ST&E) were completed for eleven (11) of the FCC's fifteen (15) major applications, including the Automated Auction System. Control weaknesses identified during the evaluations have been communicated to system owners for resolution prior to granting final certifications and accreditations.

The FCC has recently completed a number of Computer Security Desk Reference Guides that provide technical procedures for system administrators and developers as guides on implementing the information security program and practices. These include the *Security Guide for UNIX System Development and Administration*, *Identification and Authentication on FCC Computer Systems*, *Security Guide for Application and System Management Guide*, *Computer Incident Handling Guide*, and the *Computer Incident Response Team Guide*.

The Commission's IT Contingency Plan is being drafted. The plan will address resumption and continuity of services at the FCC's Portals I location, as well as the Consumer Center in Gettysburg, PA, which has been designated as the agency's hotsite. The approach has been to involve business process owners from the various bureaus as well as ITC and Consumer Center staff. Once the draft is completed, the IT Contingency Plan will be tested, finalized, and integrated with the Facility Contingency Plan to comprise an overall agency plan for continuity of services.

The Computer Security Office continues to proactively promote awareness of information security at all levels of the agency. Numerous security briefings were held throughout the year to educate program and bureau officials on information security issues. Additionally, ITC has established the Computer Security Program repository on the Commission's Intranet where FCC policies, procedures, bulletins, and alerts on protecting agency's computer resources are easily accessible to ITC staff and customers at the Portals I and Consumer Center locations.

While the Commission has implemented numerous positive controls over its computer resources, we identified areas of improvement for management, operational, and technical controls. Implementing corrective areas for identified weaknesses will increase the effectiveness of the agency's information security program and practices. As

prescribed by OMB M-02-09, "Reporting Instructions for the Government Information Security Reform Act and Updated Guidance on Security Plans of Action", a plan of action for each finding identified during the FY 2002 independent evaluation, including milestones and completion dates, should be developed by the agency. The plans should identify the corrective actions that the agency intends to take to address control areas that need strengthening and identify any obstacles which may impede correction of deficiencies noted.

The final report of detailed findings and recommendations resulting from the FY2002 GISRA independent evaluation is expected to be completed and issued by November 30, 2002.

APPENDIX A

FY 2002 Government Information Security Reform Act (GISRA) Independent Evaluation

---

Federal Communications Commission - Office of Inspector General
Responses to OMB M-02-09 GISRA Reporting Questions

The Office of Management and Budget (OMB) issued memorandum M-02-09 on July 2, 2002 as guidance to agencies on reporting the results of Fiscal Year (FY) 2002 independent evaluations performed in accordance with the Government Information Security Reform Act ("GISRA" or "the Security Act"). Included with the memorandum were questions regarding high-level management performance measures that were to be addressed by Agency Heads, Agency Program Officials, and Offices of Inspector General (IG). To that end, the Federal Communications Commission's ("FCC" or "Commission") IG, in this appendix to our report, is providing its responses to the thirteen (13) questions regarding performance measures.

The IG has based its responses on questions related to the Commission's information security program and practices on our FY 2002 independent evaluation. Other questions, not necessarily specific to the agency's information security program and practices, were addressed by obtaining information from the Commission's Information Technology Center (ITC) who worked with the appropriate agency offices to prepare responses. These questions, which were outside the scope of our independent evaluation, have not been validated by the IG. We have re-stated each question posed by OMB and provided our responses directly after each question.

I. General Overview

1. **OMB Question:**
   Identify the agency's total security funding as found in the agency's FY02 budget request, FY02 budget enacted, and the President's FY03 budget. This should include a breakdown of security costs by each major operating division or bureau and include critical infrastructure protection costs that apply to the protection of government operations and assets. Do not include funding for critical infrastructure protection pertaining to lead agency responsibilities such as outreach to industry and the public.

   FCC-IG Response:
   Per instructions issued by the Office of Management and Budget (OMB), the Office of Inspector General (IG) is not required to address this question.

2. **OMB Question:**
   Identify and describe as necessary the total number of programs and systems in the agency, the total number of systems and programs reviewed by the program officials, CIOs, or IGs in both last year's report (FY01) and this year's report (FY02) according to the format provided below. Agencies should specify whether they used the NIST self-assessment guide or an agency developed methodology. If the latter was used, confirm that all elements of the NIST guide were addressed.

FCC-IG Response:

	FY01	FY02
a. Total number of agency programs.	1	1
b. Total number of agency systems.	17	17
c. Total number of programs reviewed.	1	1
d. Total number of systems reviewed.	17 In FY01, the IG conducted a review of one (1) major application, the Consolidated Database System (CDBS). FCC's Information Technology Center (ITC) assessed general support systems and major applications through a combination of a system-wide risk analysis, a penetration test, development of security plans, and security test and evaluations on several major applications.	17 In FY02, the IG conducted a FISCAM-based review, which incorporated guidance from NIST, FIPS and other federal guidance on one (1) major application, the Automated Auctions System. ITC performed risk assessments in accordance with NIST 800-26 on all major applications and general support systems.

3. **OMB Question:**
Identify all material weakness in policies, procedures, or practices as identified and required to be reported under existing law. (Section 3534(c)(1)-(2) of the Security Act.) Identify the number of reported material weaknesses for FY 01 and FY 02, and the number of repeat weaknesses in FY02.

FCC-IG Response:

	FY01	FY02
a. Number of material weaknesses reported.	5	5
b. Number of material weaknesses repeated in FY02.		5

Sources: Report on the Federal Communications Commission Fiscal Year 2000 Financial Statement Audit, June 25, 2001. Report on the Federal Communications Commission Fiscal Year 2001 Financial Statement Audit, April 30, 2002.

II. Responsibilities of Agency Head

1. **OMB Question:**
Identify and describe any specific steps taken by the agency head to clearly and unambiguously set forth the Security Act's responsibilities and authorities for the agency CIO and program officials. Specifically how are such steps implemented and enforced? Can a major operating component of the agency make an IT investment decision without review by and concurrence of the agency CIO?

FCC-IG Response:
The FCC Chairman has specifically directed the agency Chief Information Officer (CIO) and Computer Security Officer (CSO) to act as the single points of contact for implementing the Security Act provisions and assessing compliance at all levels of the agency. While program officials are responsible for specific missions within the Bureau or Office, the CIO has been directed to centrally manage IT security for the agency. This mandate has been implemented through the assignment of a CSO and the development of a Computer Security Strategic Plan that when completed will be integrated with IT Strategic Plan. ITC has indicated that investments are required to be reviewed by, and concurred with by the agency CIO. On September 10, 2002, FCC-IG began an audit of the Commission's IT capital investment program and practices, which will, among other things, verify whether a major operating component can make IT investment decisions without the review and concurrence of the CIO.

2. **OMB Question:**
How does the head of the agency ensure that the agency's information security plan is practiced throughout the life cycle of each agency system? (Sections 3533(a)(1)(A)-(B), (b)(3)(C)-(D), (b)(6) and 3534(a)(C) of the Security Act.) During the reporting period, did the agency head take any specific and direct actions to oversee the performance of 1) agency program officials and 2) the CIO to verify that such officials are ensuring that security plans are up-to-date and practiced throughout the lifecycle of each system?

FCC-IG Response:
On November 8, 2000, the CIO and IG completed a collaborative effort that established policy and procedures for development of IT systems over the complete life cycle. The FCC Systems Development Life Cycle (SDLC) provides specific activities and tasks that must be followed in managing medium to large-scale systems. The system security plan development process was modified to specifically identify the security controls and processes to be addressed at each stage of the SDLC.

The IG is planning to conduct an audit of the SDLC policy to evaluate the implementation and adoption of the policy and its required procedures. In FY 2002, ITC conducted a review of the SDLC process as part of NIST's Self-Assessment Guide (SP 800-26) to ensure that the agency is looking at security controls during the appropriate life-cycle phase. Adjustments were made to the process and the changes were promulgated throughout the agency.

3. **OMB Question:**
How has the agency integrated its information and information technology security program with its critical infrastructure protection responsibilities, and other security programs (e.g., continuity of operations, and physical and operational security)? (Sections 3534 (a)(1)(B) and (b)(1) of the Security Act.) Does the agency have separate staffs devoted to other security programs, are such programs under the authority of different agency officials, if so what specific efforts have been taken by the agency head or other officials to eliminate unnecessary duplication of overhead costs and ensure that policies and procedures are consistent and complimentary across the various programs and disciplines?

FCC-IG Response:
For the Commission's information technology resources, physical and operational security are integrated and centrally managed under a single program. The Director of the Information Technology Center is designated as the Commission's CIO. The CIO is responsible for establishing the agency's computer security program inclusive of network and application security plans, continuity of operations/disaster recovery plans, and incident handling procedures, as well as authorizing systems to operate.

The FCC's CSO is responsible for the development, administration, and oversight of the Commission's IT security programs. Among the CSO's duties is developing and reviewing general support system and major application security plans, COOP and contingency plans, and incident handling procedures, as well as assisting the FCC bureaus/offices with IT system security program development and administration.

The CSO is in the process of drafting a Computer Security Program Strategic Plan which will be integrated with the agency's IT Strategic Plan. This plan will support the minimum essential critical programs, identify the infrastructure protection planning roles and responsibilities, provide for vulnerability assessments of Commission computer-based assets, and establish an emergency management and incident handling program, including continuity of operation and disaster recovery plans.

Additionally, the CSO has been appointed to sit on the FCC's Homeland Security Policy Council to provide a link between the agency's IT security measures and Federal Homeland Security initiatives.

Oversight of physical security of the Commission has been assigned to the Commission's Security Officer. The Security Officer is responsible for agency security operations including physical security, employee and contractor badges, lock and key services, site guard services, and a security operations center.

4. **OMB Question:**
Has the agency undergone a Project Matrix review? If so, describe the steps the agency has taken as a result of the review. If no, describe how the agency identifies its critical operations and assets, their interdependencies and interrelationships, and how they secure those operations and assets. (Sections 3535(a)(1)(A)-(B), (b)(3)(C)-(D), (b)(6) and 3534(a)(C) of the Security Act.)

FCC-IG Response:
The FCC has not undergone a Project Matrix review. However, during March 2001 a working group was formed to propose an agency definition for "major information system" and identify the FCC's major information systems from a comprehensive inventory of FCC information systems.

In January 2002, the CIO approved the following definition for major information system (MIS):

> *"…a system – either automated or manual – requiring special management attention because it meets at least one of the following attributes:*
>
> - *It has high annual or system life cost associated with its development, operations, and maintenance;*
> - *It plays a significant role in the efficient administration of the Commission's programs, finances, property, or other revenue generating programs;*
> - *It has potential to cause a high risk or harm to the Commission if its associated data were compromised."*

Using the newly approved definition, a new list of "major applications" or "major information systems" was approved by the CIO. Major applications added from the 2002 FCC IT study will be addressed as part of the FY03 security program.

5. **OMB Question:**
How does the agency head ensure that the agency, including all components, has documented procedures for reporting security incidents and sharing information regarding common vulnerabilities? Identify and describe the procedures for external reporting to law enforcement authorities and to the General Services Administration's Federal Computer Incident Response Center (FedCIRC). Identify actual performance according to the measures and the number of incidents reported in the format provided below. (Section 3534(b)(2)(F)(i)-(iii) of the Security Act.)

FCC-IG Response:

a. Total number of agency components including bureaus, field activities.	One (1)
b. Number of agency components with incident handling and response capability.	4 Computer Incidents Response Teams (CIRT)
c. Number of agency components that report to FedCIRC.	1
d. Does the agency and its major components share incident information with FedCIRC in a timely manner consistent with FedCIRC and OMB guidance?	Yes
e. What is the required average time to report to the agency and FedCIRC following an incident?	Within 24 hours
f. How does the agency, including the programs within major components, confirm that patches have been tested and installed in a timely manner?	By conducting scans using Symantec's Enterprise Security Management (ESM) assessment software.

	FY01	FY02
g. By agency and individual component, number of incidents (e.g., successful and unsuccessful network penetrations, root or user account compromises, denial of service attacks, website defacing attacks, malicious code and virus, probes and scans, password access) reported by each component.	4	3*
h. By agency and individual component, number of incidents reported externally to FedCIRC or law enforcement.	4	3*

*FCC-IG obtained documentation, which verifies the occurrence and reporting of one (1) of the three (3) incidents that occurred in FY02.

III. Responsibilities of Agency Program Officials

1. **OMB Question:**
Have agency program officials: 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? (Section 3534(a)(2) of the Security Act.)

FCC-IG Response:

COMPONENT OR BUREAU NAME	TOTAL NUMBER OF SYSTEMS
TOTAL NUMBER OF AGENCY SYSTEMS	17; 2 General Support Systems (GSS) and 15 Major Applications

OMB Question:
By each major agency component and aggregated into an agency total, from last year's report (FY01) and this reporting period (FY02) identify actual performance according to the measures and in the format provided below for the number and percentage of total systems.

FCC-IG Response:

COMPONENT OR BUREAU NAME				
	FY01 #	FY01 %	FY02 #	FY02 %
a. Systems that have been assessed for risk.	10	59%	12	71%
b. Systems that have been assigned a level of risk after a risk assessment has been conducted (e.g., high, medium, or basic).	17	100%	17	100%
c. Systems that have an up-to-date security plan.	6	11%	16	94%
d. Systems that have been authorized for processing following certification and accreditation.	0	0%	0	0%
e. Systems that are operating without written authorization (including the absence of certification and accreditation).	16	94%	17	100%
f. Systems that have the costs of their security controls integrated into the life cycle of the system.	17	100%	17	100%
g. Systems for which security controls have been tested and evaluated in the last year.	8	47%	2	12%
h. Systems that have a contingency plan.*	17	100%	2*	12%*
i. Systems for which contingency plans that have been tested in past year.*	0	0%	0*	0%*

*The FY01 GISRA independent evaluation resulted in a finding that the agency's existing contingency plans were outdated and recommended that the plans be updated. With the exception of one major application system and one general support system, during the FY02 follow-up on prior year finding it was determined that an up to date contingency plan has not

been implemented, and thus no testing had been performed. However, the agency is currently developing Information Technology continuity of operations and disaster recovery plans, which will address resumption and continuity of services for the remaining general support systems and major applications. The plan will also include requirements for conducting periodic tests of the plan.

2. **OMB Question:**
For operations and assets under their control, have agency program officials used appropriate methods (e.g., audits or inspections) to ensure that contractor provided services (e.g., network or website operations) or services provided by another agency for their program and systems are adequately secure and meet the requirements of the Security Act, OMB policy and NIST guidance, national security policy, and agency policy? Identify actual performance according to the measures and in the format provided below. (Sections 3532(b)(2), 3533(b)(2), 3534(a)(1)(B) and (b)(1) of the Security Act.)

FCC-IG Response:
External contractor or other agency services are provided by: Digital Systems Group, Mellon Bank, JPMorgan Chase Bank, Colsen Bank, Quick Hire, the National Finance Center (Department of Agriculture, New Orleans), and the National Business Center (Department of Interior, Denver).

Internal contractor services are provided by: Nova Technologies for ITC Operations, Vistronix for the Computer Resource Center, and AAC, Inc., Computech, and Zen Technologies for the Wireless Telecommunications Bureau.

COMPONENT OR BUREAU NAME		
	FY01	FY02
a. Number of contractor operations or facilities.	9	10
b. Number of contractor operations or facilities reviewed.	3	3

IV. Responsibilities of Agency Chief Information Officers

1. **OMB Question:**
Has the agency CIO: 1) adequately maintained an agency-wide security program; 2) ensured the effective implementation of the program and evaluated the performance of major agency components; and 3) ensured the training of agency employees with significant security responsibilities? Identify actual performance according to the measures and in the format provided below. (Section 3534(a)(3)-(5)) and (Section 3534(a)(3)(D), (a)(4), (b)(2)(C)(i)-(ii) of the Security Act.)

FCC-IG Response:

	FY01	FY02
a. Other than GAO or IG audits and reviews,	10	12

how many agency components and field activities received security reviews?		
b. What percentage of components and field activities has had such reviews?	59%	71%
c. Number of agency employees including contractors.	2,500	2,684
d. Number and percentage of agency employees including contractors that received security training.	700 (28%); 260 received orientation training	2,684 (100%); 287 received orientation training
e. Number of employees with significant security responsibilities.	43	59
f. Number of employees with significant security responsibilities that received specialized training.	13	18
g. Briefly describe what types of security training were available.	Orientation, Annual and Specialized Training, Seminars, Security Notices, and SANS Institute	Orientation, Annual and Specialized Training, Seminars, Security Notices, and SANS Institute
h. Total costs for providing training described in (g).	$35,500	$48,800
i. Do agency POA&Ms account for all known agency security weaknesses including of all components and field activities? If no, why not?	The quarterly POA&Ms submitted per FY01 reporting instructions did not account for all weaknesses. The agency has obtained a better understanding of the GISRA reporting requirements. Additionally, the initial POA&M did not include weaknesses that had not been issued in final audit/evaluation reports, although they were communicated as draft findings. When final reports were issued, subsequent POA&Ms were not modified to include these weaknesses. Going forward, all known weaknesses will be reflected in agency POA&Ms.	
j. Has the CIO appointed a senior agency information security official?	Yes, the FCC Computer Security Officer is the senior agency information security official.	

2. **OMB Question:**

For operations and assets under their control (e.g., network operations), has the agency CIO used appropriate methods (e.g., audits or inspections) 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? Identify actual performance according to the measures and in the format provided below. (Sections 3532(b)(2), 3533(b)(2), 3534(a)(1)(B) and (b)(1) of the Security Act.)

FCC-IG Response:

	FY01	FY02
a. Number of contractor operations or facilities.	9	10
b. Number of contractor operations or facilities reviewed.	3	3

3. **OMB Question:**

Has the agency CIO fully integrated security into the agency's capital planning and investment control process? Were security requirements and costs reported on every FY03 capital asset plan (as well as in the exhibit 53) submitted by the agency to OMB? If no, why not? Identify actual performance according to the measures and in the format provided below. (Sections 3533(a)(1)(A)-(B), (b)(3)(C)-(D), (b)(6) and 3534(a)(C) of the Security Act.)

FCC-IG Response:

	FY03 Budget Materials	FY04 Budget Materials
a. Number of capital asset plans and justifications submitted to OMB?	2	5
b. Number of capital asset plans and justifications submitted to OMB without requisite security information and costs?	0	0
c. Were security costs reported for all agency systems on the agency's exhibit 53?	yes	yes
d. Have all discrepancies been corrected?	N/A	N/A
e. How many have the CIO/other appropriate official independently validated prior to submittal to OMB?	2*	5*

*FCC-IG will review this information as part of the OIG's IT Capital Investment Audit that began on September 10, 2002.

APPENDIX B

FY 2002 Government Information Security Reform Act (GISRA) Independent Evaluation

---

Federal Communications Commission - Office of Inspector General

Report on Automated Auction System
(Audit Report No. 02-AUD-02-08)

(Previously posted on OIG Website)