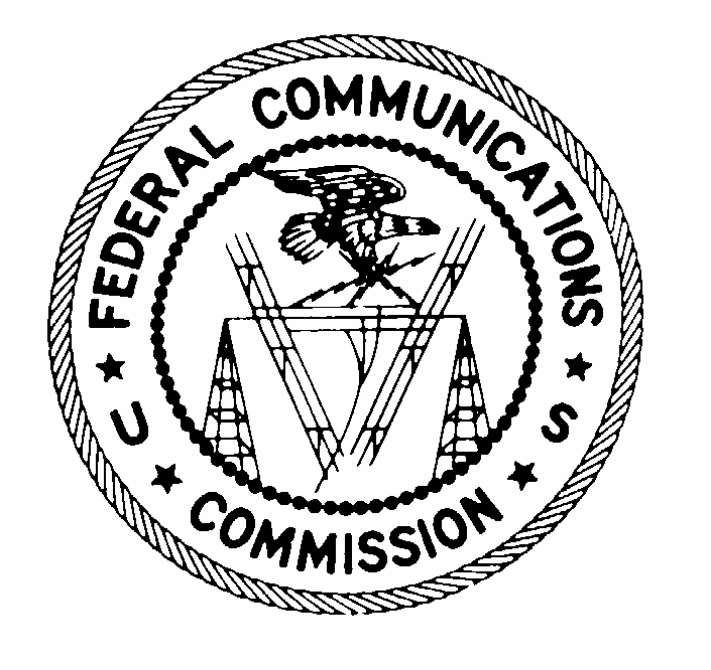
Federal Communications Commission
Office of Inspector General



FY 2003 Federal Information Security Management Act (FISMA) Independent Evaluation

September 22, 2003

TABLE OF CONTENTS

		Page
EXECUTIVE SUMMARY		2
BACKGROUND		3
OBJECTIVE		3
SCOPE		4
RESULTS OF FISCAL YEAR 2003 INDEPENDENT EVALUATIONS		5
APPENDIX A	OIG Responses to OMB M-03-19 GISRA Reporting Questions	A-1
APPENDIX B	Report on Follow-up Audit of Computer Controls at the FCC Consumer Center (Audit Report No. 01-AUD-07-30)	B-1

Executive Summary

The Federal Information Security Management Act ('FISMA' or 'the Act') was signed into law on December 17, 2002 as Title III, "Information Security", of the E- Government Act of 2002. The Act permanently re-authorizes the framework established by the Government Information Security Reform Act (GISRA), which expired in November 2002.

FISMA requires all federal agency heads to transmit to the Office of Management and Budget (OMB) an annual agency report consisting of separate components prepared by the agency Chief Information Officer (CIO) and the Office of Inspector General (IG). A key provision of the Act also requires that the agency IG, or independent evaluators designated by the IG, perform an annual independent evaluation of the agency's information security program and practices. For fiscal year (FY) 2003, the Federal Communications Commission's ("Commission" or "FCC") IG engaged KPMG, LLP to conduct its independent evaluation.

The overall objective of the FISMA independent evaluation was to evaluate the effectiveness of the Commission's information security program. Generally, we found the Commission's information technology security to be effective. We used the National Institute of Standards and Technology (NIST) "Self-Assessment Guide for Information Technology Systems (Self-Assessment Guide 800-26)" as a basis for our methodology to assess the risk for each component of the FCC's program. As applicable, additional guidance was received from methodology provided in the Federal Information Systems Control Audit Manual (FISCAM), as well as other laws and directives related to management and protection of Federal information resources.

This year's independent evaluation included an assessment of the agency's Plan of Actions and Milestones (POA&M) process and an aging study. The aging study was performed to identify the length of time that POA&M weaknesses remain open and determine how effective the agency is in implementing corrective actions. We noted that the FCC effectively monitors and tracks all known weaknesses via the POA&M. However, only one-third of the corrective actions are completed on track and 63% have experienced or are experiencing delays. Our study identified that significant delays are encountered when implementing defined corrective actions.

OMB Memoranda M-03-19 dated August 6, 2003 entitled, "Reporting Instructions for the Federal Information Security Management Act and Updated Guidance of Quarterly IT Security Reporting" was followed to perform and report the results of our independent evaluation. Appendix A provides the IG's responses to OMB's questions that address high-level performance measures of the FCC's information security program and practices. We plan to issue the final detailed findings and recommendations from this year's FISMA independent evaluation by November 30, 2003.

FISMA also requires that IGs select an appropriate subset of business applications for independent review. Our Follow-up Audit of Computer Controls at the FCC Consumer Center and FY 2003 Audit of Revenue Accounting and Management Information System (RAMIS) Application Controls satisfy this requirement. Appendix B forwards the final report on our Follow-up Audit of Computer Controls at the FCC Consumer Center (Audit Report No. 01-AUD-07-30). The audit of RAMIS application and security controls has been substantially completed. A final report of detailed findings and recommendations is planned for November 30, 2003.

Background

The Federal Information Security Management Act (hereafter referred to as 'FISMA' or 'the Act') was signed into law on December 17, 2002 as Title III, "Information Security" of the Electronic Government Act of 2002. FISMA permanently re-authorizes the framework established by the Government Information Security Reform Act (GISRA), which expired in November 2002. The requirements of the Act apply to all federal agencies.

The Act requires each federal agency head to transmit to the Director of the Office of Management and Budget (OMB) an annual report of high-level performance measures on its information security program. The agency report consists of two separate components that are prepared by the agency Chief Information Officer (CIO) and the Office of Inspector General (IG). The CIO's report provides the results of annual system and program reviews as well progress in implementing the agency's POA&Ms. The IG's report summarizes the results of independent evaluations performed during the fiscal year and the agency's progress in implementing Plans of Actions & Milestones (POA&M).

A key provision of the Act requires that the agency Office of Inspector General (IG), or independent evaluators designated by the IG, perform an annual independent evaluation of the agency's information security program and practices. For fiscal year (FY) 2003, 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.

OMB Memoranda M-03-19 dated August 6, 2003 and entitled, "Reporting Instructions for the Federal Information Security Management Act and Updated Guidance of Quarterly IT Security Reporting", was followed to perform and report the results of our independent evaluation.

Evaluation Objective

The objectives of the current year's FISMA independent evaluation and risk assessment were to:

1. Evaluate the effectiveness of the Commission's information security program through the use of FISMA security assessment tools.

2. Prepare the annual submission in accordance with the reporting requirements mandated by OMB Memorandum M-03-19, dated August 6, 2003 and entitled, "Reporting Instructions for the Federal Information Security Management Act and Updated Guidance of quarterly IT Security Reporting."

3. Follow-up on the findings identified during the FY 2001 and FY 2002 GISRA reviews that are documented in prior FCC IG audit reports (Report Nos. 01-AUD-11-43 and 02-AUD-02-06).

To accomplish the objectives of the review we specifically included the following tasks:

    1. Review documentation and interview communication, developers, and system management personnel to obtain an understanding of the IT structure and operational environment;

2. Design and conduct tests appropriate for a FISMA review. For FY 2003 these tests included:
    a. A review of the Commission's Plans of Action and Milestones, POA&Ms, to determine if POA&Ms include all findings.
    b. An aging of POA&M findings to determine the length of time vulnerabilities have remained open.
    c. An analysis of the FCC's process for testing for vulnerabilities to determine if the FCC has a process to test for significant information security vulnerabilities on a systematic basis.
    d. An assessment of the FCC's certification and accreditation (C&A) process.
    e. An aging of completed C&As to determine how long C&As operate under interim authority to operate at the FCC.

3. Review the effectiveness of application security for a sample of applications;

4. Classify and rank security risk areas and vulnerabilities;

5. Make recommendations for specific improvements to security, as appropriate; and

6. Identify areas for review in subsequent years.

Evaluation Scope

The scope of our independent evaluation included the security infrastructure managed by the Office of Managing Director's (OMD) Information Technology Center (ITC) and the Auctions Automation Branch of the Commission's Wireless Telecommunications Bureau (WTB).

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."
- FCC Instruction 1479.2, "Computer Security Program Directive."
- NIST Special Publication 800-37, entitled "Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems", October 2002 (DRAFT).

FISMA also requires that IGs select an appropriate subset of business applications for independent review. Our Follow-up Audit of Computer Controls at the FCC Consumer Center and FY 2003 Audit of Revenue Accounting and Management Information System (RAMIS) Application Controls satisfy this requirement. The report on the results of the Consumer Center follow-up audit is included with this report as Appendix B. The audit of RAMIS application and security controls has been substantially completed. A final report of detailed findings and recommendations is planned for November 30, 2003.

Results of FY2003 IG Independent Evaluations

The FCC continues to make progress in strengthening its information security program. In the current fiscal year the FCC's Computer Security Program revised its methodology for certifying and accrediting its major applications and general support systems. The revised methodology is designed to more effectively identify and address risks and ensure the security of resources in the operational environment. Specific accomplishments in the current fiscal year include the following:

- Security tests and evaluation (ST&Es) were re-performed for 53% of the agency's major applications and general support systems.

- Eight (8) systems were authorized for processing following certification and accreditation. At the close of the prior year none of the Commission's systems had been certified and accredited.

While these efforts demonstrate the Commission's commitment to information security, the lack of an IT Continuity of Operation Plan (COOP) represents a risk to the security posture of the agency. Completion of the overall ITC COOP, which is in draft, will further strengthen the FCC's information security program. The FCC has contracted an outside vendor to assist with the development of the plan, which will address all major applications and general support systems. However, the plan is significantly behind schedule.

Additional observations of the Commission's information security program identified during FY2003 IG independent evaluations are discussed below. Some observations are specific to the overall security program, while others address specific systems and information resources.

FY2003 FISMA Independent Evaluation and Risk Assessment

The IG has prepared responses to OMB's questions that report upon high-level performance measures of the Commission's information security program and practices. The responses are based upon the results of our FY 2003 independent evaluation. Some questions were not necessarily specific to the agency's information security program addressed by the scope of our audit. In these cases, we have relied upon information provided by the appropriate agency bureaus and offices. The IG accepted the information provided without performing further validation. Appendix A to this report provides the IG's annual submission of responses to OMB questions in the required format.

Our current year FISMA independent evaluation of the FCC's information security program will result in a detailed report that will (1) identify and rank the critical security risk factors, and (2) provide observations and recommendations for improvements to the agency's information security program, if any. The assessment is substantially complete and the final report is

expected to be issued by November 30, 2003.

Included as a component of the FY2003 independent evaluation was an evaluation of the agency's POA&M process and an aging study. The aging study was performed to identify the length of time that POA&M weaknesses remain open and how effective the agency is in implementing corrective actions for identified deficiencies. Included in the scope of the aging study were current fiscal year and all prior year quarterly POA&Ms issued by the FCC. On a positive note, the Commission has corrected last year's Government Information Security Reform Act (GISRA) independent evaluation finding that reported that not all known weaknesses were included in the agency POA&Ms. Additionally, FCC management has appropriately outlined corrective actions for remediation of each weakness reported in the POA&Ms.

While FCC management continues to effectively monitor and track the progress of the corrective actions planned for all known security weaknesses, the results of our aging study indicate that the timely remediation of weaknesses should be improved upon. The summary of our aging study is provided in the following table:

Summary of POA&M Aging Study		
	# Weaknesses	**% Weaknesses**
Total Number of Weakness Reported by Agency POA&Ms	**48**	**100%**
Number of Corrective Actions Completed On Time	16	33%
Number of Corrective Actions Delayed and Completed	10	21%
Number of Corrective Actions that are On-going and On-track for Remediation	2	4%
Number of Corrective Actions Delayed and Not Completed	20	42%
Delays Encountered	**# Weaknesses**	**% Weaknesses**
1-3 months	4	13%
6 – 12 months	13	43%
13 – 18 months	10	33%
19 – 24 months	1	3%
Over 24 months	2	7%

As indicated above, very few corrective actions designed to correct security weaknesses are completed on track. Our study identified that significant delays are encountered when implementing defined corrective actions. In total, 48 weaknesses have been reported by the agency POA&Ms. Corrective actions have been reported as completed on time for 16 (33%)of reported weaknesses and 2 (4%) were reported as on track for completion. Of the total security weaknesses for which POA&Ms have been developed, corrective actions for 30 (63%) have experienced or are experiencing delays. Implementation of planned corrective actions were delayed between 1 and 3 months for 4 (13%) of the identified weaknesses; 13 (43%) were delayed between 6 and 12 months; 10 (33%) were delayed between 13 and 18 months; and 3 (10%) were delayed between 19 and 24 months.

Follow-up Audit on Computer Controls as the FCC Consumer Center

We performed a follow-up audit on Audit Report No. 00-AUD-01-12 dated June 21, 2001 entitled "Report on Audit of Computer Controls at the FCC National Call Center." The original report noted that significant technical control and internal control improvements could be made to improve the overall security posture of the Consumer Center (formerly known as the National Call Center). The original report contained one hundred three (103) specific findings.

The objective of our recent follow-up audit was to determine the status of sixty-six (66) of the original one hundred three (103) conditions. Specifically excluded were conditions from the original audit related to physical security and other conditions determined by the IG to be outside the scope of the audit. The guideline for performing this audit was the Federal Information System Control Audit Manual (FISCAM). Additional guidance was received from the National Institute of Standards and Technology (NIST) and other laws and directives related to management and protection of Federal information resources including the FCC's "Computer Security Program Directive" (FCC Instruction 1479.2).

Of the sixty-six (66) conditions that were reviewed, the audit identified twenty-one (21) conditions with an 'open' status, forty-five (45) with a 'closed' status, and four (4) new control weaknesses. Represented in the open conditions were twenty (20) that had been reported as resolved by FCC management prior to the audit. From our review we ascertained that some of these conditions had to be re-opened for reasons including the degradation of security controls after initial corrective actions were taken, introduction of new hardware which may not have been properly configured, or subsequent changes made by personnel with administrative and maintenance duties. As we conducted the follow-up audit and identified open conditions, FCC management took proactive measures to initiate resolution of findings that remained open.

The final report (Audit Report No. 01-AUD-07-30) issued from the follow-up audit is attached as Appendix B to this submission.

FY2003 Audit of RAMIS Application Controls

In the current fiscal year, we initiated an audit of the application and security controls over the Commission's RAMIS application. RAMIS is the Commission's internal revenue management system that supports application and regulatory fee accounting, spectrum auction loan portfolio management, accounting for auction proceeds, accounting for enforcement actions, and other accounts receivable.

The objective of this audit was to determine the extent and effectiveness of RAMIS application and security controls. The audit has been substantially completed and is in progress. During the audit we noted several positive observations as summarized below:

- The FCC's Computer Security Program office conducted a physical security review of the contractor's facility. In response to observations of security controls at the facility, FCC management took appropriate action to improve the security of the RAMIS production and test servers.

- No vulnerabilities were identified during a limited external penetration testing of the application and related network devices included in the scope the assessment.

- RAMIS passwords are being encrypted.

- Strong root passwords are in use on the production server and the administrative workstation.

The final report will include and discuss weaknesses in the areas of audit trails, user account and password management, segregation of duties, and contractor oversight. The details of weakness identified and corresponding recommendations will be released in the final audit report expected to be issued by November 30, 2003.

FCC's timely implementation of corrective actions to remediate the weaknesses identified by our FY 2003 independent evaluations and previous audits and special reviews will increase the effectiveness of the agency's information security program and practices. As prescribed by OMB Memoranda M-03-19 dated August 6, 2003 and entitled, "Reporting Instructions for the Federal Information Security Management Act and Updated Guidance of Quarterly IT Security Reporting", POA&Ms for each vulnerability identified should be developed with milestones, completion dates, and budget resources required to implement corrective actions. Finally the agency should continue to actively report on and monitor the correction of vulnerabilities through the POA&M process.

APPENDIX A

FY 2003 Federal Information Security Management Act (FISMA) Independent Evaluation

---

Federal Communications Commission - Office of Inspector General

Responses to OMB Memorandum M-03-19 FY2003 FISMA Reporting Questions

A.1. Identify the agency's total IT security spending and each individual major operating division or bureau's IT security spending as found in the agency's FY03 budget enacted. This should 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.

Bureau Name	FY03 IT Security Spending ($ in thousands)
Federal Communications Commission (FCC)	$4,100
Agency Total	$4,100

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

	FY03 Programs		FY03 Systems		FY03 Contractor Operations or Facilities	
Bureau Name	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number *	Number Reviewed
Office of the Inspector General	1	1	19	2	6	1
Office of the Managing Director	1	1	19	19	6	0
Agency Total	**1**	**1**	**19**	**19**	**6**	**0**

b. For operations and assets under their control, have agency program officials and the agency CIO used appropriate methods (e.g., audits or inspections) to ensure that contractor provided services or services provided by another agency for their program and systems are adequately secure and meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy?	Yes	X	No	
c. If yes, what methods are used? If no, please explain why.	The FCC Computer Security Officer (CSO) has performed a FISMA program review of the Office of the Managing Director's (OMD) Information Technology Center (ITC) using the NIST Self-Assessment Guide.			
d. Did the agency use the NIST self-assessment guide to conduct its reviews?	Yes	X	No	
e. If the agency did not use the NIST self-assessment guide and instead used an agency developed methodology, please confirm that all elements of the NIST guide were addressed in the agency methodology.	Yes	N/A	No	

* - Total based on external contract entities that process FCC data at an offsite location. This total includes Digital Systems Group, Mellon Bank, JP Morgan/Chase Bank, Colsen Bank, The National Finance Center, and The National Business Center.

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

	FY03 Material Weaknesses			
Bureau Name	Total Number	Total Number Repeated from FY02	Identify and Describe Each Material Weakness	POA&Ms developed? Y/N
Federal Communications Commission	3	3	Lack of compliance with OMB Circular A-130 Requirement for a Comprehensive Security Plan. Inadequacies and Inconsistencies in the Mainframe and Network and Network Access Request Process. The FCC does not possess an Information Technology Center (ITC) Contingency or Disaster Recovery Plan.	Y
Agency Total	3	3		

Sources: Report on the Federal Communications Commission Fiscal Year 2001 Financial Statement Audit, April 30, 2002. Report on the Federal Communications Commission Fiscal Year 2002 Financial Statements Audit, January 31, 2003

A.4. This question is for IGs only. Please assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestone process that meets the criteria below. Where appropriate, please include additional explanation in the column next to each criteria.	**Yes**	**No**
Agency program officials develop, implement, and manage POA&Ms for every system that they own and operate (systems that support their programs) that has an IT security weakness.	Yes	
Agency program officials report to the CIO on a regular basis (at least quarterly) on their remediation progress.	Yes	
Agency CIO develops, implements, and manages POA&Ms for every system that they own and operate (systems that support their programs) that has an IT security weakness.	Yes	
The agency CIO centrally tracks and maintains all POA&M activities on at least a quarterly basis.	Yes	
The POA&M is the authoritative agency and IG management tool to identify and monitor agency actions for correcting information and IT security weaknesses.		No - The FCC's OMD has established responsibility for audit follow-up within the agency's Performance Evaluation and Records Management (PERM) division under OMB Circular A-50 guidelines. Treating the POA&M as the IG tool for tracking IT security findings would create parallel systems that duplicate the same function. FCC-OIG submitted comments on the draft FY03 FISMA guidelines to OMB by e-mail. In the e-mail, FCC-OIG noted this long-standing practice of the Commission and requested of OMB that security guidance allow flexibility for other offices within an agency to be the authority for managing IT findings.
System-level POA&Ms are tied directly to the system budget request through the IT business case as required in OMB budget guidance (Circular A-11) to tie the justification for IT security funds to the budget process.	Yes - FY2004 business cases identified the anticipated spending on IT security, including the correction of identified weaknesses as well as other IT-security costs. Beginning with FY2005, in accordance with FISMA POA&M guidelines, agency POA&Ms will include the amount of funding resources identified in IT business cases.	

A.4. This question is for IGs only. Please assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestone process that meets the criteria below. Where appropriate, please include additional explanation in the column next to each criteria.	**Yes**	**No**
Agency IGs are an integral part of the POA&M process and have access to agency POA&Ms.		No - Weakness identified during IG audits are incorporated into the agency POA&Ms however, quarterly POA&Ms where not distributed to the FCC IG during the fiscal year.
The agency's POA&M process represents a prioritization of agency IT security weaknesses that ensures that significant IT security weaknesses are addressed in a timely manner and receive, where necessary, appropriate resources.		No - Agency POA&Ms are not being prioritized to identify significant IT security weaknesses.

B.1. Identify and describe any specific steps taken by the agency head to clearly and unambiguously set forth FISMA's responsibilities and authorities for the agency CIO and program officials. Specifically how are such steps implemented and enforced?	The FCC Chairman has specifically directed the agency Chief Information Officer (CIO) to appoint the CSO to act as the single point 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 of 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 Program Plan, which when completed will supplement the Information Technology Center Strategic Plan. The CSO is also responsible for developing and maintaining the system security plan for each major application and general support system to support each FCC Bureau and Office.
B.2. Can a major operating component of the agency make an IT investment decision without review by and concurrence of the agency CIO?	No - We noted during our audit of the Auctions IT capital investment practices, beginning with the FY 2003 Auctions budget request, the FCC began managing the Auctions cost budget development process in a similar fashion to the overall appropriated budget process for the agency. In July of 2002, the FCC finalized its Information Technology (IT) Strategic Plan. This plan provides a high-level framework for the Commission's IT capital investment process.
B.3. How does the head of the agency ensure that the agency's information security plan is practiced throughout the life cycle of each agency system?	The FCC Systems Development Life Cycle (SDLC) provides specific activities and tasks that must be followed in managing medium to large-scale systems. The SDLC process was modified to specifically identify security controls and processes to be addressed at each stage of the SDLC, including system security plan development, security test and evaluation, and certification and accreditation.
B.4. During the reporting period, did the agency head take any specific and direct actions to oversee the performance of 1) agency program officials and 2) the CIO to verify that such officials are ensuring that security plans are up-to-date and practiced throughout the lifecycle of each system?	During FY 2003 the FCC CSO performed a FISMA self-assessment review of the FCC ITC. This review focused on the managerial, operational, and technical aspects of the FCC's information technology security.
B.5. Has the agency integrated its information and information technology security program with its critical infrastructure protection responsibilities, and other security programs (e.g., continuity of operations, and physical and operational security)?	For the Commission's information technology resources, physical and operational security are integrated and centrally managed under a single program. The Director of the ITC 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.
B.6. Does the agency have separate staffs devoted to other security programs, are such programs under the authority of different agency officials, if so what specific efforts have been taken by the agency head or other officials to eliminate unnecessary duplication of overhead costs and ensure that policies and procedures are consistent and complimentary across the various programs and disciplines?	The FCC is an independent agency of the United States Federal Government and reports directly to congress. Within this agency is the ITC, which supports the Information Technology related needs its mission and employees. A sub-department of the ITC is the Computer Security Program (CSP), which provides an agency-wide Information Technology security function for the entire agency. The 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 syste and major application security plans, Continuity of Operations Plan (COOP) and contigency plans, and incident handling procedures, as well as assisting the FCC bureaus and offices with IT system security program development and administration. 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. The FCC Wireless Telecommunication Bureau Auctions Automation Branch also has one staff-member responsible for reviewing security on the Auction general support system and on all Auctions related major application. This staff person is independent of the FCC CSO. The Auctions Operations Branch has in place a contract with a third party responsible for outsourced, off-hours intrusion detection within the Auctions general support system.

B.7. Identification of agency's critical operations and assets (both national critical operations and assets and mission critical) and the interdependencies and interrelationships of those operations and assets.				
a. Has the agency fully identified its critical operations and assets, including their interdependencies and interrelationships?	Yes	X	No	
b. If yes, describe the steps the agency has taken as a result of the review.	The FCC CSO has performed a FISMA self-assessment of the ITC in order to identify all critical operations and assets.			
c. If no, please explain why.				

B.8. How does the agency head ensure that the agency, including all components, has documented procedures for reporting security incidents and sharing information regarding common vulnerabilities?

The FCC developed a Computer Incident Response Guide that contains specific response instructions, a standardized form for reporting incidents, and guidance for reporting outside of the agency. The report form used in the guide was modeled after the FedCIRC and FBI-NIPC formats. This form includes a section for sharing information outside of the agency.

The FCC has also formed a Computer Incident Response Team (CIRT). The team's focal point is the mitigation of impact from computer related incidents at the Commission. The team is comprised of technical experts in the fields of personal computing, network design and functionality, telecommunications, application development and management, and security and investingations. The CIRT is broken into 4 sub-teams comprised of individuals from the Applications Integrations Group (AIG), the Network Development Group (NDG), the Operations Group (OG), and the Auctions Operational Branch (Auctions).

a. Identify and describe the procedures for external reporting to law enforcement authorities and to the Federal Computer Incident Response Center (FedCIRC).	The CSO serves as the principal contact for the FCC CIRT. To support information sharing, the CSO reports to, and works closely with, the CIO, the Federal Computer Incident Response Capability (FedCIRC) managed by the GSA, the FBI - National Infrastructure Protection Center (FBI - NIPC), and the Computer Emergency Response Team (CERT) at Carnegie Melon University, as well as others.			
b. Total number of agency components or bureaus.	17			
c. Number of agency components with incident handling and response capability.	3			
d. Number of agency components that report to FedCIRC.	1			
e. Does the agency and its major components share incident information with FedCIRC in a timely manner consistent with FedCIRC and OMB guidance?	Yes			
f. What is the required average time to report to the agency and FedCIRC following an incident?	24 Hours			
g. How does the agency, including the programs within major components, confirm that patches have been tested and installed in a timely manner?	The FCC uses custom scripts, developed by the Application Integrations Group (AIG), to ensure that all systems are using the most current and up-to-date patches. The level of system patching is also reviewed for each major application and general support system during the Security Test and Evaluation (ST&E) portion of the system's Certification and Accreditation (C&A) examination.			
h. Is the agency a member of the Patch Authentication and Distribution Capability operated by FedCIRC?	Yes		No	X
i. If yes, how many active users does the agency have for this service?	N/A			
j. Has the agency developed and complied with specific configuration requirements that meet their own needs?	Yes	X	No	
k. Do these configuration requirements address patching of security vulnerabilities?	Yes	X	No	

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

Bureau Name	Number of incidents reported	Number of incidents reported externally to FedCIRC or law enforcement
Federal Communications Commission	A total of 27 incidents were reports in FY 2003.	Three of the 27 incidents were reported to FedCIRC in FY 2003.

C.1. Have agency program officials and the agency CIO: 1) assessed the risk to operations and assets under their control; 2) determined the level of security appropriate to protect such operations and assets; 3) maintained an up-to-date security plan (that is practiced throughout the life cycle) for each system supporting the operations and assets under their control; and 4) tested and evaluated security controls and techniques? By each major agency component and aggregated into an agency total, identify actual performance in FY03 according to the measures and in the format provided below for the number and percentage of total systems.

Bureau Name	Total Number of Systems	Number of systems assessed for risk and assigned a level or risk		Number of systems that have an up-to-date IT security plan		Number of systems certified and accredited		Number of systems with security control costs integrated into the life cycle of the system		Number of systems for which security controls have been tested and evaluated in the last year		Number of systems with a contingency plan *		Number of systems for which contingency plans have been tested *	
		No. of Systems	% of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Federal Communications Commission	19	10	53%	19	100%	8	42%	19	100%	10	53%	1	5%	1	5%
Agency Total	**19**	**10**	**53%**	**19**	**100%**	**8**	**42%**	**19**	**100%**	**10**	**53%**	**1**	**5%**	**1**	**5%**

* - Denotes the FCC Auctions COOP, which only covers the Automated Auctions System (AAS).

C.2. Identify whether the agency CIO has adequately maintained an agency-wide IT security program and ensured the effective implementation of the program and evaluated the performance of major agency components.	
Has the agency CIO maintained an agency-wide IT security program? Y/N	Yes, FCC Directive FCCINST 1479.2 serves as the overall FCC-wide IT Security Program. This plan has been approved by the FCC CIO and has been given a 5 year lifespan. The plan will expire in October 2006.
Did the CIO evaluate the performance of all agency bureaus/components? Y/N	Yes
How does the agency CIO ensure that bureaus comply with the agency-wide IT security program?	The FCC CSO has performed an review of the FCC using the NIST Self-Assessment Guide.
Has the agency CIO appointed a senior agency information security officer per the requirements in FISMA?	An FCC CSO and Deputy CSO have been appointed by the FCC CIO.
Do agency POA&Ms account for all known agency security weaknesses including all components?	Yes

C.3. Has the agency CIO ensured security training and awareness of all agency employees, including contractors and those employees with significant IT security responsibilities?							
Total number of agency employees in FY03	Agency employees that received IT security training in FY03		Total number of agency employees with significant IT security responsibilities	Agency employees with significant security responsibilities that received specialized training		Briefly describe training provided	Total costs for providing training in FY03
	Number	Percentage		Number	Percentage		
2582	2582	100%	64	56	88%	The FCC ITC and the CSP provide initial security awareness for general and detailed security related topics. The CSP also develops and teaches quarterly IT security briefs on topics relevant to the FCC. In addition, the CSP develops IT security notices and bulletins, which are posted on the FCC Intranet site.	$26,000

C.4. Has the agency CIO fully integrated security into the agency's capital planning and investment control process? Were IT security requirements and costs reported on every FY05 business case (as well as in the exhibit 53) submitted by the agency to OMB?

Bureau Name	Number of business cases submitted to OMB in FY05	Did the agency program official plan and budget for IT security and integrate security into all of their business cases? Y/N	Did the agency CIO plan and budget for IT security and integrate security into all of their business cases? Y/N	Are IT security costs reported in the agency's exhibit 53 for each IT investment? Y/N
Federal Communications Commission	6	Yes, the total dollar amount for IT security is noted in each business case.	Yes, a percentage of the funding dedicated to IT security for each function is denoted in each business case.	Yes, a percentage of the funding dedicated to IT security for each function is denoted in the overall agency-wide OMB 53.

Quarterly POA&M Updated Information	Programs	Systems
a. Total number of weaknesses identified at the start of the quarter.	N/A*	N/A*
b. Number of weaknesses for which corrective action was completed on time (including testing) by the end of the quarter.	N/A*	N/A*
c. Number of weaknesses for which corrective action is ongoing and is on track to complete as originally scheduled.	N/A*	N/A*
d. Number of weaknesses for which corrective action has been delayed including a brief explanation for the delay.	N/A*	N/A*
e. Number of new weaknesses discovered following the last POA&M update and a brief description of how they were identified (e.g., agency review, IG evaluation, etc.).	N/A*	N/A*

* - FISMA Guidance provide by OMB does not require agency OIGs to complete this section

Quarterly IT Security Performance Measures Update															
Bureau Name	**Total Number of Systems**	**Number of systems assessed for risk and assigned a level or risk**		**Number of systems that have an up-to-date IT security plan**		**Number of systems certified and accredited**		**Number of systems with security control costs integrated into the life cycle of the system**		**Number of systems for which security controls have been tested and evaluated in the last year**		**Number of systems with a contingency plan**		**Number of systems for which contingency plans have been tested**	
		No. of Systems	% of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Federal Communications Commission	19	10	53%	19	100%	8	42%	19	100%	10	53%	5	26%	0	0%
Agency Total	**19**	**10**	**53%**	**19**	**100%**	**8**	**42%**	**19**	**100%**	**10**	**53%**	**5**	**26%**	**0**	**0%**