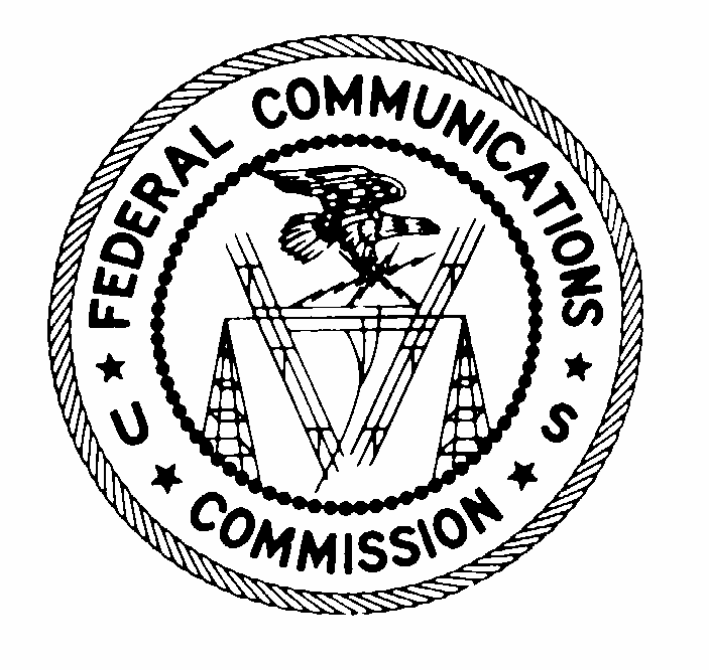
Federal Communications Commission
Office of Inspector General



FY 2004 Federal Information Security Management Act (FISMA) Independent Evaluation

October 6, 2004

TABLE OF CONTENTS

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) 2004, 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.

OMB Memoranda M-04-25 dated August 23, 2004 entitled, "FY 2004 Reporting Instructions for the Federal Information Security Management Act" 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. Appendix B provides the final report for our FY 2004 FISMA Independent Evaluation and Risk Assessment (Audit Report No. 04-AUD-06-08).

FISMA also requires that IGs select an appropriate subset of business applications for independent review. The results of our FY 2003 Audit of Revenue Accounting and Management Information System (RAMIS) Application Controls (Audit Report No. 03-AUD-01-01), included as Appendix C, satisfies this requirement. Appendix D is the report on the FY 2003 FISMA Independent Evaluation and Risk Assessment (Audit Report No. 03-AUD-06-09). Appendix E forwards the final memo on our Disaster Recovery Plan Survey (Audit Report No. 03-AUD-12-27).

APPENDIX A

FY 2004 Federal Information Security Management Act (FISMA) Independent Evaluation

---

Federal Communications Commission - Office of Inspector General

Responses to OMB Memorandum M-04-25 FY 2004 FISMA Reporting Questions

2004 FISMA Report

Agency:	Federal Communications Commission
Date Submitted:	10/6/2004
Submitted By:	OIG

Contact Information:

Name:	Walker Feaster
E-mail:	walker.feaster@fcc.gov
Phone:	(202) 418-0476

Section A: System Inventory and IT Security Performance
NOTE: ALL of Section A should be completed by BOTH the Agency CIO and the OIG.

A.1. By bureau (or major agency operating component), identify the total number of programs and systems in the agency and the total number of contractor operations or facilities. The agency CIOs and IG's shall each identify the total number that they reviewed as part of this evaluation in FY04. NIST 800-26, is to be used as guidance for these reviews.

A.2. For each part of this question, identify actual performance in FY04 for the total number of systems by bureau (or major agency operating component) in the format provided below.

	A.1						A.2									
	A.1.a. FY04 Programs		**A.1.b. FY04 Systems**		**A.1.c. FY04 Contractor Operations or Facilities**		**A.2.a. Number of systems certified and accredited**		**A.2.b. Number of systems with security control costs integrated into the life cycle of the system**		**A.2.c. Number of systems for which security controls have been tested and evaluated in the last year**		**A.2.d. Number of systems with a contingency plan**		**A.2.e. Number of systems for which contingency plans have been tested**	
Bureau Name	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
Federal Communications Commission	1	1	19	19	5	0	19	100.0%	19	100.0%	19	100.0%	6	31.6%	6	31.6%
Agency Total	**1**	**1**	**19**	**19**	**5**	**0**	**19**	**100.0%**	**19**	**100.0%**	**19**	**100.0%**	**6**	**31.6%**	**6**	**31.6%**

Comments:

A.1.c - The total number of contractor operations or facilities in FY 2004 is 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, The National Finance Center, and The National Business Center.

A.2.d - The total number of systems with a contingency plan in FY 2004 includes the FCCNET network environment, the Access Control System, as well as the Commission's internal supporting infrastructure for FFS and FPPS, which is identified in the FCC Information Technology Disaster Recover Plan. Also included within this total is the Wireless Telecommunication Bureau Auctions Network and Automated Auctions System, which are noted in the Auction Continuity of Operations Plan.

A.3	
A.3. Evaluate the degree to which the following statements reflect the status in your agency, by choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the Comment area provided below.	
Statement	**Evaluation**
a. Agency program officials and the agency CIO have used appropriate methods 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.	Almost Always, or 96-100% of the time
b. The reviews of programs, systems, and contractor operations or facilities, identified above, were conducted using the NIST self-assessment guide, 800-26.	Mostly, or 81-95% of the time
c. In instances where the NIST self-assessment guide was not used to conduct reviews, the alternative methodology used addressed all elements of the NIST guide.	Rarely, or 0-50% of the time
d. The agency maintains an inventory of major IT systems and this inventory is updated at least annually.	Almost Always, or 96-100% of the time
e. The OIG was included in the development and verification of the agency's IT system inventory.	Almost Always, or 96-100% of the time
f. The OIG and the CIO agree on the total number of programs, systems, and contractor operations or facilities.	Almost Always, or 96-100% of the time
g. The agency CIO reviews and concurs with the major IT investment decisions of bureaus (or major operating components) within the agency.	Almost Always, or 96-100% of the time
Statement	**Yes or No**
h. The agency has begun to assess systems for e-authentication risk.	Yes
i. The agency has appointed a senior agency information security officer that reports directly to the CIO.	Yes

Comments:

Item A - Each agency or contractor that provides a service to the Commission is required, by contract, to follow the guidance outlined by FCC Directive FCCINST 1479.2 and to review and sign a copy of the FCC Rules of Behavior. These documents establish security requirements for all FCC systems.

Item B - Onsite reviews of three of the contractor facilities that house FCC major application where not performed during FY 2004.

Item C - The Computer Security Program did not use any methodology other than the NIST self-assessment guide to conduct reviews during the fiscal year.

Section B: Identification of Significant Deficiencies
NOTE: ALL of Section B should be completed by BOTH the Agency CIO and the OIG.

B.1. By bureau, identify all FY 04 significant deficiencies in policies, procedures, or practices required to be reported under existing law. Describe each on a separate row, and identify which are repeated from FY03. In addition, for each significant deficiency, indicate whether a POA&M has been developed. Insert rows as needed.

B.1.

Bureau Name	FY04 Significant Deficiencies			
	Total Number	Total Number Repeated from FY03	Identify and Describe Each Significant Deficiency	POA&M developed? Yes or No
Federal Communications Commission	2	2	1. Compliance with OMB Circular No. A-130 Requirements for a Comprehensive Security Plan (Modified Repeat Condition)	Yes
			2. Accelerate Efforts to Develop and Test FCC's Contigency Plans (Modified Repeat Condition).	Yes
Agency Total	**2**	**2**		

Comments:

Section C: OIG Assessment of the POA&M Process
NOTE: Section C should *ONLY* be completed by the OIG. The CIO should leave this section blank.

C.1. Through this question, and in the format provided below, assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestone (POA&M) process. This question is for IGs only. Evaluate the degree to which the following statements reflect the status in your agency by choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the Comment area provided below.

C.1	
Statement	**Evaluation**
a. Known IT security weaknesses, from all components, are incorporated into the POA&M.	Almost Always, or 96-100% of the time
b. **Program officials** develop, implement, and manage POA&Ms for systems they own and operate (systems that support their program or programs) that have an IT security weakness.	Almost Always, or 96-100% of the time
c. Program officials report to the CIO on a regular basis (at least quarterly) on their remediation progress.	Almost Always, or 96-100% of the time
d. **CIO** develops, implements, and manages POA&Ms for every system they own and operate (a system that supports their program or programs) that has an IT security weakness.	Almost Always, or 96-100% of the time
e. CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	Almost Always, or 96-100% of the time
f. The POA&M is the authoritative agency **and** IG management tool to identify and monitor agency actions for correcting information and IT security weaknesses.	Almost Always, or 96-100% of the time
g. 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).	Almost Always, or 96-100% of the time
h. OIG has access to POA&Ms as requested.	Almost Always, or 96-100% of the time
i. OIG findings are incorporated into the POA&M process.	Almost Always, or 96-100% of the time
j. POA&M process prioritizes IT security weaknesses to help ensure that significant IT security weaknesses are addressed in a timely manner and receive appropriate resources.	Rarely, or 0-50% of the time

Comments:

Regarding Item J - Agency POA&Ms are not being prioritized to identify significant IT security weaknesses.

C.1 OIG Assessment of the Certification and Accreditation Process
Section C should only be completed by the OIG. OMB is requesting IGs to assess the agency's certification and accreditation process in order to provide a qualitative assessment of this critical activity. This assessment should consider the quality of the Agency's certification and accreditation process. Any new certification and accreditation work initiated after completion of NIST Special Publication 800-37 should be consistent with NIST Special Publication 800-37. This includes use of the FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems," to determine an impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans. Earlier NIST guidance is applicable to any certification and accreditation work completed or initiated before finalization of NIST Special Publication 800-37. Agencies were not expected to use NIST Special Publication 800-37 as guidance before it became final.

Statement	Evaluation
Assess the overall quality of the Agency's certification and accreditation process. Comments: The FCC's Information Technology Center's Computer Security Program (CSP) uses the guidance provided in NIST Special Publication 800-37 as the primary basis for its certification and accreditation methodology. The methodology also incorporates NIST Special Publication 800-26 for additional guidance. Prior to the final release of NIST Special Publication 800-37, the CSP was utilizing NIST Special Publication 800-26, FIPS 199, as well as the draft NIST Special Publication 800-37 for guidance in the FCC certification and accreditation process. At the close of FY 2004, all of the FCC's major applications and general support systems had been certified to operate on the network. To date, five (5) of the FCC's nineteen (19) major applications and general support systems, including the Equipment Authorization System, the Experimental Licensing Systems, and the Universal Licensing System have been certified to operate using the finalized NIST Special Publication 800-37.	Excellent

	We reviewed all C&A packages during our FISMA independent evaluation and risk assessment. We noted that the FCC's process relies on a relatively high level of technical expertise to test system controls and ensure that risks posed by major applications and or general support systems are identified and properly mitigated. To ensure that risks are adequately identified, the process includes security testing consisting of vulnerability assessments and penetration tests. During security testing, the CSP used various automated tools to identify security weaknesses. This testing yielded a number of significant technical issues including those associated with patch management, operating system configuration, and database audit settings. We noted that all findings were properly communicated to system owners and either resolved during the certification and accreditation process or, depending of the level of risk associated, agreed to be resolved in the near future. This was evident in the certification and accreditation statements for the Equipment Authorization System, the Auctions Network, and the International Bureau Filing System.	

Section D
NOTE: ALL of Section D should be completed by BOTH the Agency CIO and the OIG.

D.1. First, answer D.1. If the answer is yes, then proceed. If no, then skip to Section E. For D.1.a-f, identify whether agencywide security configuration requirements address each listed application or operating system (Yes, No, or Not Applicable), and then evaluate the degree to which these configurations are implemented on applicable systems. **For example:** If your agency has a total of 200 systems, and 100 of those systems are running Windows 2000, the universe for evaluation of degree would be 100 systems. If 61 of those 100 systems follow configuration requirement policies, and the configuration controls are implemented, the answer would reflect "yes" and "51-70%". If appropriate or necessary, include comments in the Comment area provided below.

D.2. Answer Yes or No, and then evaluate the degree to which the configuration requirements address the patching of security vulnerabilities. If appropriate or necessary, include comments in the Comment area provided below.

D.1. & D.2.

	Yes, No, or N/A	Evaluation
D.1. Has the CIO implemented agencywide policies that require detailed specific security configurations and what is the degree by which the configurations are implemented?		
a. Windows XP Professional	N/A	
b. Windows NT	N/A	
c. Windows 2000 Professional	Yes	Almost Always, or 96-100% of the time
d. Windows 2000	N/A	
e. Windows 2000 Server	Yes	Almost Always, or 96-100% of the time
f. Windows 2003 Server	N/A	
g. Solaris	Yes	Almost Always, or 96-100% of the time
h. HP-UX	N/A	
i. Linux	N/A	
j. Cisco Router IOS	No	Rarely, or 0-50% of the time
k. Oracle	No	Rarely, or 0-50% of the time
l. Other. Specify: Silicon Graphics IRIX	No	Rarely, or 0-50% of the time
	Yes or No	**Evaluation**
D.2. Do the configuration requirements implemented above in D.1.a-f., address patching of security vulnerabilities?	Yes	Almost Always, or 96-100% of the time

Comments:
Item J - Cisco does not provide patches for the IOS. All vulnerabilities are mitigated and/or corrected via upgrades of the IOS Software
Item I - The Linux operating system is present within the FCC's environment, however its use is limited to application testing purposes.
Item K - The FCC Financial Operations Group also manages an Oracle Data Warehouse that serves as a repository of Federal Financial System (FFS) data. However, this system is not considered a major application and is not managed under the Office of the Chief Information Officer. As such, it is not included in this listing.
Item K and L - These platforms are managed by an external contractor and are not connected directly to the internal FCC network environment. However, the contractor has not developed a configuration guide for either the Oracle or IRIX platforms.

Section E: Incident Detection and Handling Procedures
NOTE: ALL of Section E should be completed by BOTH the Agency CIO and the OIG.

E.1. Evaluate the degree to which the following statements reflect the status at your agency. If appropriate or necessary, include comments in the Comment area provided below.

E.1

Statement	Evaluation
a. The agency follows documented policies and procedures for reporting incidents internally.	Almost Always, or 96-100% of the time
b. The agency follows documented policies and procedures for external reporting to law enforcement authorities.	Almost Always, or 96-100% of the time
c. The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov	Almost Always, or 96-100% of the time

E.2.

E.2. Incident Detection Capabilities.

	Number of Systems	Percentage of Total Systems
a. How many systems underwent vulnerability scans and penetration tests in FY04?	11	58%

b. Specifically, what tools, techniques, technologies, etc., does the agency use to mitigate IT security risk?

Answer:

The FCC Information Technology Center utilizes various hardware and software based solutions to mitigate IT security risks both internal and external to the Commission. Cisco PIX and Checkpoint firewalls control and monitor traffic entering and exiting the FCC's network environment. Also utilized are network segmentation and layering, controlled network routing, host and network-based virus protection software, system log monitoring and alert monitoring. The FCC ITC also implemented various intrusion detection solutions, including ISS RealSecure and TripWire. Lastly, the FCC ITC Computer Security Program (CSP) conducts periodic security tests and evaluations to identify and mitigate risks.

Comments:

Section G: Training
NOTE: ALL of Section G should be completed by BOTH the Agency CIO and the OIG.

G.1. Has the agency CIO ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities? If appropriate or necessary, include comments in the Comment area provided below.

G.1.

G.1.a. Total number of employees in FY04	G.1.b. Employees that received IT security awareness training in FY04, as described in NIST Special Publication 800-50		G.1.c. Total number of employees with significant IT security responsibilities	G.1.d. Employees with significant security responsibilities that received specialized training, as described in NIST Special Publications 800-50 and 800-16		G.1.e. Briefly describe training provided	G.1.f. Total costs for providing IT security training in FY04 (in $'s)
	Number	Percentage		Number	Percentage		
2443	2443	100%	75	40	53%	- FCC's Top 10 SANS Vulnerabilities - IT DRP Overview and Training - CRC Computer Security (CS) Training - New Staff CS Orientation Training - Monthly CS Notices - CS Alerts and Advisories - Other Specialized IT Security Training - Other Ad-hoc Security Briefings	$159,055.37

	Yes or No
a. Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training?	Yes

Comments:
The total number of employees in field G.1.a is the sum of the total number of full time employees (2016) and total number of contractors with network access (427).

Section F: Incident Reporting and Analysis
NOTE: ALL of Section F should be completed by BOTH the Agency CIO and the OIG.

F.1. For each category of incident listed: identify the total number of successful incidents in FY04, the number of incidents reported to US-CERT, and the number reported to law enforcement. If your agency considers another category of incident type to be high priority, include this information in category VII, "Other". If appropriate or necessary, include comments in the Comment area provided below

F.2. Identify the **number of systems** affected by each category of incident in FY04. If appropriate or necessary, include comments in the Comment area provided below.

F.1., F.2. & F.3.

	F.1. Number of Incidents, by category:			F.2. Number of systems affected, by category, on:		
	F.1.a Reported internally	F.1.b. Reported to US-CERT	F.1.c. Reported to law enforcement	F.2.a. Systems with complete and up-to-date C&A	F.2.b. Systems without complete and up-to-date C&A	F.2.c. How many successful incidents occurred for known vulnerabilities for which a patch was available?
	Number of Incidents	Number of Incidents	Number of Incidents	Number of Systems Affected	Number of Systems Affected	Number of Systems Affected
I. Root Compromise	0	0	0	0	0	0
II. User Compromise	1	0	0	0	0	0
III. Denial of Service Attack	0	0	0	0	0	0
IV. Website Defacement	0	0	0	0	0	0
V. Detection of Malicious Logic	0	0	0	0	0	0
VI. Sucessful Virus/worm Introduction	1	0	0	0	0	0
VII. Other	2	0	0	2	0	0
Totals:	4	0	0	2	0	0

Comments:

Item II was the result of a user account being compromised on a local workstation and the deletion of data contained on the hard drive.

Item VI was the result of the Beagle Worm infecting a limited number of workstations in the FCC environment. The vendor delayed the release of the software patch, thus resulting in the infection.

Item VII was the result of a distruption of email services due to a high number of emails being received by the Commission and the uploading of an unauthorized wet page to an FCC external web server.

APPENDIX B

FY 2004 Federal Information Security Management Act (FISMA) Independent Evaluation

---

Federal Communications Commission - Office of Inspector General

FY 2004 Federal Information Security Management Act (FISMA) Independent Evaluation and Risk Assessment (Audit Report No. 04-AUD-06-08)

APPENDIX C

FY 2004 Federal Information Security Management Act (FISMA) Independent Evaluation

---

Federal Communications Commission - Office of Inspector General

FY 2003 Audit of Revenue Accounting & Management Information System (RAMIS) Application Controls (Audit Report No. 03-AUD-01-01)

APPENDIX D

FY 2004 Federal Information Security Management Act (FISMA) Independent Evaluation

---

Federal Communications Commission - Office of Inspector General

FY 2003 Federal Information Security Management Act (FISMA) Independent Evaluation and Risk Assessment (Audit Report No. 03-AUD-06-09)

APPENDIX E

FY 2004 Federal Information Security Management Act (FISMA) Independent Evaluation

---

Federal Communications Commission - Office of Inspector General
FY 2004 Disaster Recovery Plan Survey
(Audit Report No. 03-AUD-12-27)