OFFICE OF INSPECTOR GENERAL

MEMORANDUM

DATE: February 6, 2004

TO: Chairman

FROM: Inspector General

SUBJECT: Report on Fiscal Year 2003 Federal Information Security Management Act (FISMA) Evaluation and Risk Assessment

The Office of Inspector General (OIG) has completed its annual evaluation of the Commission's Information Security program in accordance with the Federal Information Security Management Act (FISMA). FISMA requires that Inspectors General, or the independent evaluators they choose, perform an annual evaluation of each agency's information security program and practices. We contracted with KPMG, LLP to perform the independent evaluation. On September 22, 2003, we issued a report, entitled "FY 2003 Federal Information Security Management Act (FISMA) Independent Evaluation," summarizing the results of our independent evaluation. As a result of the independent evaluation, we have concluded that the Commission has a generally effective information security program with acceptable practices for managing and safeguarding the Federal Communications Commission's (FCC's) information technology assets. Our report, comprised of an executive summary and an independent evaluation, was included in a package of information provided by the Commission to the Office of Management and Budget (OMB) on September 22, 2003.

However, during the independent evaluation, we identified areas for improvement in the FCC's information security management, operational and technical controls. The evaluation identified seven (7) new findings in the areas of management, operational, and technical controls. Additionally, we determined that eight (8) of the conditions identified during the FY 2002 and FY 2001 Government Information Security Reform Act (GISRA) evaluations had not been fully corrected at the time of audit fieldwork. Of these eight (8) outstanding conditions, three (3) were originally classified as High Risk. In our opinion, implementation of our recommendations and correction of the prior year conditions will strengthen the security of the Commission's information security program.

I have attached a copy of our report, entitled "FY 2003 Federal Information Security Management Act (FISMA) Independent Evaluation and Risk Assessment," (Report No. 03-AUD-06-09) summarizing the findings that resulted from our evaluation of the Commission's information security program. This report is a byproduct of the independent evaluation required by FISMA.

Our recommendations will correct present problems and minimize the risk that future security problems will occur in the FCC's information security program. All recommendations contained in the attached report will be tracked for reporting purposes by the OIG. Appendix A, Summary of Findings, provides a summary of the findings from this review. Appendix B, Detailed Findings and Recommendations, details the findings and recommendations from the review. .

On December 22, 2003, we provided a draft to the Office of Managing Director (OMD) for their review and comments. In its response dated January 16, 2004, OMD indicated concurrence with six (6) of the seven (7) new findings and seven (7) of the eight (8) of conditions identified during the FY 2002 and FY 2001 GISRA evaluations. For two (2) conditions, OMD indicated partial concurrence. For all findings, OMD outlined the corrective action taken and/or a milestone schedule for implementation of corrective action. We have included a copy of the response from OMD in its entirety as Appendix C to this report.

Due to the sensitive nature of the information contained in the appendices, we have marked them all "Non-Public – For Internal Use Only" and have limited distribution. Those persons receiving this report are requested not to photocopy or otherwise distribute this material.

If you have any questions, please contact Thomas Cline, Assistant Inspector General for Audits at (202) 418-7890.

H. Walker Feaster III

Attachment

cc: Chief of Staff
Managing Director
Chief Information Officer
Computer Security Officer, ITC
AMD-PERM

Federal Communications Commission
Office of Inspector General

FY 2003 Federal Information Security Management Act Independent Evaluation and Risk Assessment

Report No. 03-AUD-06-09

February 6, 2004

TABLE OF CONTENTS

[redacted] The Federal Information Security Management Act ("FISMA" or "the Security Act") was signed into law on December 17, 2002 as Title III, "Information Security", of the E-Government Act of 2003. FISMA permanently reauthorized the framework established by the Government Information Security Reform Act (GISRA), which expired in November 2002.

A key provision of FISMA requires that the agency Office of Inspector General (OIG), or designated independent evaluators, perform an annual review of the agency's information security program and practices. For fiscal year (FY) 2003, the Federal Communications Commission's ("the Commission" or "FCC") OIG engaged KPMG, LLP to conduct its independent evaluation and risk assessment.

The scope of the review included the security infrastructures managed by the Office of Managing Director's (OMD) Information Technology Center (ITC) and the Auctions Operations Branch of the Wireless Telecommunications Bureau (WTB). Our approach included analyzing documentation, interviewing personnel responsible for the security and administration of information resources, conducting automated scans of network devices, and reviewing previously performed audits and special reviews. During the review, we also followed up on the status of corrective actions for FY 2001 and FY 2002 GISRA findings and performed an aging analysis of quarterly Plans of Actions and Milestones (POA&Ms). Audit fieldwork was performed at the FCC's Portals facility located in Washington D. C. from July 23, 2003 through October 10, 2003.

The objective of the current year's FISMA review was to evaluate the effectiveness of the Commission's information security program. Our review included, but was not limited to, security policies, security architecture, business continuity, security capital planning, critical infrastructure, and security program planning and management.

The framework for our methodology was provided by the "Self-Assessment Guide for Information Technology Systems (Self-Assessment Guide)" issued by the National Institute of Standards and Technology (NIST). As appropriate, guidance prescribed by the "Federal Information System Controls Audit Manual (FISCAM)" was used. Guidance was also obtained from additional NIST publications, other laws and directives pertaining to the protection of Federal information resources, and agency-specific guidance.

The Office of Management and Budget's (OMB) Memoranda M-03-19, entitled "Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting" was followed to perform and report upon the results of our independent evaluation. The instructions posed several questions regarding high-level management performance measures that were to be addressed by Agency Heads, Agency Program Officials, and agency OIGs. A separate

report with responses to the questions asked of agency OIGs was prepared and submitted on September 22, 2003 to OMB with the Commission's FY 2003 FISMA Submission.

Overall, we determined that the FCC continues to demonstrate dedication to improving and maintaining the protection of its information assets. Notably, the Computer Security Program (CSP) has dedicated resources and worked in concert with other groups within ITC to evaluate and implement controls to strengthen the effectiveness of information security. During our evaluation, we noted several positive security controls as well as well as areas where improved controls are recommended.

Appendices A and B to this report provide the details of the observations and conditions identified during our FY 2003 independent evaluation and risk assessment. Recommendations are provided for FCC management consideration. Specifically, we identified seven (7) new findings in the areas of management, operational, and technical controls. Additionally, we determined that five (5) of the conditions identified during the FY 2001 GISRA evaluation and three (3) from the FY 2002 GISRA evaluation had not been fully corrected at the time of audit fieldwork. Of these eight (8) outstanding conditions, three (3) were originally classified as High Risk.

Through our aging analysis of quarterly POA&Ms, we concluded the FCC effectively tracks and monitors corrective actions of known security weaknesses. However, we determined that the process for the timely correction of identified security weaknesses could be improved upon. While corrective action plans have been developed for all weaknesses identified through audits and other reviews, a large percentage of corrective actions experience slippage in their implementation dates.

As stated in the FY 2002 GISRA final report, we commend FCC management for documenting procedures that are repeatable and consistent. Again, we re-emphasize this year that FCC management within ITC ensure that full time employees and contractors properly implement required security measures at the operational level.

On December 22, 2003, we provided a draft to the Office of Managing Director (OMD) for their review and comments. In its response dated January 16, 2004, the Office of Managing Director (OMD) indicated concurrence with six (6) of the seven (7) new findings and seven (7) of the eight (8) of conditions identified during the FY 2002 and FY 2001 GISRA evaluations. For two (2) conditions, OMD indicated partial concurrence. For all findings, OMD outlined the corrective action taken and/or a milestone schedule for implementation of corrective action. We have included a copy of the response from OMD in its entirety as Appendix C to this report.

Due to the sensitive nature of the information contained in the appendices, we have marked them all "Non-Public – For Internal Use Only" and have limited distribution. Those persons receiving this report are requested not to photocopy or otherwise distribute this material.

[redacted] The Federal Information Security Management Act ("FISMA" or "the Security Act") was signed into law on December 17, 2002 as Title III, *"Information Security"*, of the E-Government Act of 2003. The Security Act permanently reauthorized the framework established by the Government Information Security Reform Act (GISRA), which expired in November 2002.

A key provision of FISMA requires that the agency Office of Inspector General (OIG), or designated independent evaluators, perform an annual evaluation of the agency's information security program and practices. For fiscal year (FY) 2003, the Federal Communications Commission's ("the Commission" or "FCC") OIG engaged KPMG, LLP to conduct the agency's risk assessment and independent evaluation.

The framework for our methodology was provided by the "Self-Assessment Guide for Information Technology Systems (Self-Assessment Guide)" issued by the National Institute of Standards and Technology (NIST). As appropriate, guidance prescribed by the "Federal Information Systems Control Audit Manual (FISCAM)" was used. Guidance was also obtained from additional NIST publications, as well as other laws and directives pertaining to the protection of Federal information resources as listed below, including agency-specific guidance. The primary guidelines used in the course of this review are as follows:

- The E-Government Act of 2002, Public Law 107-347, enacted on December 17, 2002
- 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-97-16, entitled "Information Technology Architectures"
- OMB M-97-02, entitled "Funding Information Systems Investments"
- OMB M-03-19, "Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting" (August 6, 2003)
- OMB M-02-09, "Reporting Instructions for the Government Information Security Reform Act and Updated Guidance on Security Plans of Action and Milestones" (July 2, 2002)
- FCC INST 1479.2 "Computer Security Program Directive."
- NIST Special Publication 800-37, "Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems"(October 2002, Draft)

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

(GAGAS).

[redacted] 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 specific objectives of the evaluation were to:

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 FISMA security assessment tools to evaluate the effectiveness of the Commission's information security program.

4. Prepare the annual submission in accordance with the reporting requirements mandated under FISMA for FY 2003. In addition to preparing the annual submission, the contractor was tasked with providing a detailed report to (1) identify and rank the critical security risk factors and (2) document observations and recommendations for improvements, if any.

5. Follow-up on audit findings from the FY 2001 and FY 2002 GISRA reviews documented by FCC-OIG report numbers 01-AUD-11-43 and 02-AUD-02-06.

[redacted] The scope of our independent evaluation and risk assessment included the security infrastructures managed by the Office of Managing Director's Information Technology Center (ITC) and the Auctions Operations Branch of the Commission's Wireless Telecommunications Bureau (WTB).

The FY 2003 FISMA audit 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. The review also followed up on the status of corrective actions for FY 2001 and FY 2002 GISRA findings and an aging analysis of quarterly Plans of Actions and Milestones (POA&Ms).

The Security Act also requires that the OIG select an appropriate subset of agency applications for review. Our *Follow-up Audit of Computer Controls at the FCC Consumer Center* satisfies this requirement for the current year. The results of this audit can be found in OIG Report No. 01-AUD-07-30, which was forwarded with the Commission's FY 2003 FISMA Submission to OMB on September 22, 2003.

Our observations from the independent evaluation and risk assessment 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 were:

- 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 were:

- Identification and Authentication
- Audit Trails
- Logical Access Controls

Each finding has been further categorized by risk ratings of 'High', 'Medium', or 'Low'. In assigning ratings, we considered whether each condition, if exploited, could result in misuse or loss FCC data, as well as the potential degree of exposure to the Commission. Risk categories are defined below:

High Risk:	A security risk which can cause a business disruption, if exploited. The identified condition presents a level of risk that requires immediate and appropriate redress by FCC management. To not do so would have the potential effect of increasing the risks of unnecessary system downtime, misuse and destruction/exposure of critical FCC data.
Medium Risk:	A security risk in conjunction with other events, which can cause a business disruption, if exploited. It is important for FCC management to take appropriate corrective action on these medium-risk security control conditions in order to protect the integrity, availability, and confidentiality of FCC data.
Low Risk:	A security risk which may cause operational annoyances, if exploited.

[redacted] During our FISMA review we assessed 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. Audit fieldwork was conducted from July 23, 2003 through October 10, 2003 at the FCC's Portals headquarters located in Washington, DC.

Overall, we determined that the FCC continues to demonstrate dedication to improving and maintaining the protection of its information assets. Notably, the Computer Security Program (CSP) has dedicated resources and worked in concert with other groups within ITC to evaluate and implement controls to strengthen the effectiveness of information security. During our evaluation, we noted several positive security controls as well as well as areas where improved controls are recommended.

Positive security controls related to the FCC's information security program and practices that were identified during the current fiscal year's independent evaluation include the following:

- The FCC's revised certification and accreditation (C&A) methodology is in compliance with recommended NIST guidance (SP 800-37, *"Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems")*.
- Security tests and evaluations (ST&Es) were re-preformed for 53 % of the agency's major applications and general support systems.

- Eight (8) systems, representing 42% of all major applications and general support systems, were authorized for processing following C&As. At the close of the prior fiscal year, none of the Commission's systems had been fully accredited and authorized to operate.

- Configuration management plans for major applications managed by the Applications Integration Group (AIG) were completed during the fourth quarter of the fiscal year.

Since the FY 2001 GISRA evaluation, the Commission has developed and/or revised numerous policies, procedures, and guides that outline specific requirements for the protection of information resources by system administrators, developers, and FCC users. As stated in the FY 2002 GISRA final report, we commend FCC management for documenting procedures that are repeatable and consistent. However, during our assessment of security controls, we noted specific instances where FCC guidance published to address prior year GISRA findings are not being followed or are not known of by the individuals responsible for implementing prescribed security measures. This was particularly noted during our review of user account management and auditing practices. As a result, we re-emphasize this year that FCC management must ensure that staff and contractors responsible for implementing all new and updated policies, procedures, and guidelines are made aware of requirements. Further, documented evidence of adherence to security requirements should be maintained and reviewed periodically by FCC management to ensure security practices are being properly conducted.

While the Commission has implemented numerous positive controls over its computer resources, we identified areas for improvement for management, operational, and technical controls. Specifically, seven (7) new findings resulted from the current year's independent evaluation and risk assessment. The findings consist of one (1) related to management controls, two (2) related to operations controls, and four (4) related to technical controls. Of the seven (7) new findings, one (1) of the conditions has been classified as 'High' risk and six (6) have been classified as 'Medium' risk.

Based upon our follow-up on FY 2001 GISRA observations, we determined that corrective actions have not been fully implemented for five (5) findings. Additionally, three (3) findings from the FY 2002 GISRA evaluation were determined to be

unresolved. Of these eight (8) outstanding conditions, three (3) were originally classified as High Risk.

Also included as a component of the FY2003 FISMA audit, was an evaluation of the agency's POA&M process and an aging study of the resolution of security weaknesses. 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 GISRA finding that reported that not all known weaknesses were included in the agency POA&Ms. Additionally, FCC management has appropriately outlined corrective actions for the 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 can be improved upon. The summary of our aging study is provided in the following table:

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%
1-3 months	4	13%
4 – 6 months	7	23%
7 – 12 months	6	20%
13 – 18 months	10	33%
19 – 24 months	1	3%
Over 24 months	2	7%

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 sixteen (33%) of the reported weaknesses and two (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 four (4) (13%) of the identified weaknesses; seven (7) (23%) were delayed between 4 and 6 months; six (6) (20%) were delayed between 7 and 12 months; ten (10) (33%) were delayed between 13 and 18 months; and three (3) (10%) were delayed between 19 and 24 months.

Appendix A provides the Summary of Findings from the FY 2003 FISMA review. Appendix B is a report of Detailed Findings and Recommendations, which outlines detailed information on the conditions identified, criteria used to evaluate the condition, effect, and recommendation(s). Both appendices identify new conditions that resulted from the current year's review as well as conditions from the FY 2001 and FY 2002 GISRA reviews that were noted with an *'open'* status.

As prescribed by OMB M-03-19, "Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting", FCC management should develop individual POA&Ms for correcting each new finding identified during this year's FISMA independent evaluation. Each corrective action should include milestones, completion dates, and the resources required to implement remedial measures.

On December 22, 2003, we provided a draft to the Office of Managing Director (OMD) for their review and comments. In its response dated January 16, 2004, the Office of Managing Director (OMD) indicated concurrence with six (6) of the seven (7) new findings and seven (7) of the eight (8) of conditions identified during the FY 2002 and FY 2001 GISRA evaluations. For two (2) conditions, OMD indicated partial concurrence. For all findings, OMD outlined the corrective action taken and/or a milestone schedule for implementation of corrective action. We have included a copy of the response from OMD in its entirety as Appendix C to this report.

This report contains non-public information. In accordance with the Commission's directive on the Management of Non-Public Information (FCCINST 1139), we have classified all appendices as "Non-Public – For Internal Use Only." Recipients of this report are expected to follow the established policies and procedures for managing and safeguarding the non-public information contained in this report as outlined in FCCINST 1139.