OFFICE OF INSPECTOR GENERAL

MEMORANDUM

DATE: September 20, 2004

TO: Chairman

FROM: Inspector General

SUBJECT: Report on Fiscal Year 2004 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 FISMA evaluation.

In our determination, the FCC continues to demonstrate a commitment to protecting federal information resources and data of the Commission. During our evaluation, we noted several positive security controls related to the FCC's information security program, including:

- Ninety percent (90%) of the Commission's major applications and general support systems have been certified to operate. By comparison, at the close of FY 2003, only eight (8) or 42% of the systems had been certified to operate.

- The FCC has strong controls regarding the back up of critical Commission data, specifically with the dual-redundancy built into the FCC's Storage Area Network (SAN) environment.

During the independent evaluation, we identified areas for improvement in the FCC's information security management, operational and technical controls. The evaluation identified one (1) new finding in the area of operational 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. We did not review the status of outstanding conditions from the FY 2003 FISMA review.

We are addressing the conditions identified during this audit in the attached report. I have attached a copy of our report, entitled "FY 2003 Federal Information Security Management Act (FISMA) Independent Evaluation and Risk Assessment," (Report No. 04-AUD-06-08) 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.

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.

On August 31, 2004, we provided a draft to the Office of Managing Director (OMD) for review and comments. In its response dated September 17, 2004, OMD indicated concurrence with the one (1) new finding in FY 2004, and seven (7) of the eight (8) conditions identified during the FY 2002 and FY 2001 GISRA evaluations. On one finding, no audit follow-up was performed. 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.

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
Director, Office of Engineering and Technology
Chief Information Officer
Computer Security Officer, ITC
AMD-PERM

Federal Communications Commission
Office of Inspector General

FY 2004 Federal Information Security Management Act Independent Evaluation and Risk Assessment

Report No. 04-AUD-06-08

September 20, 2004

TABLE OF CONTENTS

EXECUTIVE SUMMARY

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) 2004, 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, 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. Audit fieldwork was conducted from March 11, 2004 through July 6, 2004 at the FCC's Portals headquarters located in Washington, DC and Laurel Labs in Laurel, Maryland.

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 will be prepared and submitted with the Commission's FY 2004 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 and reviewed during our FY 2004 independent evaluation and risk assessment. Recommendations are provided for consideration by FCC management.

Specifically, we identified one (1) new finding in the area of operational controls. This finding has been classified as Medium Risk. 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. We did not review the status of outstanding conditions from the FY 2003 FISMA review.

On August 31, 2004, we provided a draft to the Office of Managing Director (OMD) for review and comments. In its response dated September 17, 2004, OMD indicated concurrence with the one (1) new finding in FY 2004, and seven (7) of the eight (8) conditions identified during the FY 2002 and FY 2001 GISRA evaluations. On one finding, no audit follow-up was performed. 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.

BACKGROUND

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) 2004, 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)"
- Office of Management and Budget (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"
- Draft FY 04 "Updated Reporting Instructions for FISMA and Guidance on Quarterly IT Security Reporting"
- OMB M-03-19, "Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting" (August 6, 2003)
- 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).

OBJECTIVE Our objective was to evaluate the effectiveness of the Commission's information security program by assessing the risk for each component of the program. The 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 2004. In addition to preparing the annual submission, provide 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.

Specific recommendations, as warranted, have been developed to address any internal control deficiencies identified during the conduct of review fieldwork.

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

The FY 2004 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).

Follow-up on new findings reported by the FY 2003 FISMA review was not included in the current year's scope of work due to the accelerated start date of this year's FISMA review in support of the financial statement audit reporting requirements. To provide

OMD adequate time to implement corrective actions on FY 2003 findings, follow-up on these will be included in the next year's FISMA evaluation.

The Security Act also requires that the OIG select an appropriate subset of agency applications for review. Our *FY 2003 Audit of Revenue Accounting & Management Information System (RAMIS) Application Controls* satisfies this requirement for the current year. The results of this audit can be found in OIG Report No. 03-AUD-01-01, which will be forwarded with the Commission's FY 2004 FISMA Submission to OMB.

Our observations from the independent evaluation and risk assessment have been organized according to the NIST control areas of management, operational, 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 of 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.

AUDIT OBSERVATIONS

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 March 11, 2004 through July 6, 2004 at the FCC's Portals headquarters located in Washington, DC and Laurel Labs in Laurel, Maryland.

In our determination, the FCC continues to demonstrate a commitment to protecting federal information resources and data of the Commission. During our evaluation, we

noted several positive security controls related to the FCC's information security program and practices:

- Ninety percent (90%) of the Commission's major applications and general support systems have been certified to operate. By comparison, at the close of FY 2003, eight (8) or 42% of the systems had received an authority to operate (ATO). At the time of our audit, only two (2) systems were awaiting an ATO.

- The *ITC's Disaster Recovery Plan* has been finalized and included as Appendix F of the *FCC Facilities Continuity of Operations Plan (COOP).*

- Neither the ITC nor WTB Auctions Automation Branch experienced computer security incidents due to improperly configured or improperly patched web presence and/or internal infrastructure hosts in FY 2004.

- The FCC has strong controls regarding the back up of critical Commission data, specifically with the dual-redundancy built into the FCC's Storage Area Network (SAN) environment.

- The CSP regularly communicates computer security information to all FCC users. These communications discuss practices for safeguarding information resources, threats to computer security, and educational topics related to computer security.

While the Commission has implemented numerous positive security controls over its computer resources, we identified an area for improvement. Specifically, the evaluation identified one (1) new finding in the area of operational controls.

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, four (4) as 'Medium' risk, and one (1) as 'Low' risk. We did not review the status of outstanding conditions from the FY 2003 FISMA review.

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.

On August 31, 2004, we provided a draft to the Office of Managing Director (OMD) for

review and comments. In its response dated September 17, 2004, OMD indicated concurrence with the one (1) new finding in FY 2004, and seven (7) of the eight (8) conditions identified during the FY 2002 and FY 2001 GISRA evaluations. On one finding, no audit follow-up was performed, due to timing issues. During the FY 2003 FISMA Review, we noted that COALS was not in compliance with the FCC SDLC Methodology. Because to the timing of the FY 2004 FISMA Review, we were unable to follow up with COALS project personnel for a status of the system's compliance with the FCC SDLC Methodology. However, the status will be followed up on during the FY 2005 FISMA Review. 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.