OFFICE OF INSPECTOR GENERAL

MEMORANDUM

DATE: January 6, 2003

TO: Chairman

FROM: Inspector General

SUBJECT: Report on Government Information Security Reform Act Evaluation - Findings and Recommendations

The Office of Inspector General (OIG) has completed an evaluation of the Commission's Information Security program in accordance with the Government Information Security Reform Act (Security Act). The Security Act 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 16, 2002, we issued a report, entitled "FY 2002 Government Information Security Reform Act (GISRA) 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 16, 2002.

During the independent evaluation, we identified areas for improvement in the FCC's information security management, operational and technical controls. The evaluation identified eight (8) findings in the areas of management, operational, and technical controls. Additionally, we determined that eight (8) of the conditions identified during the FY 2001 GISRA evaluation had not been fully corrected at the time of audit fieldwork. In our opinion, implementation of our recommendations and correction of the conditions identified in the FY 2001 evaluation report will strengthen the security of the Commission's information security program. These findings are addressed in the attached report, entitled "Report on FY 2002 Government Information Security Reform Act Risk Assessment and Evaluation," (Report No. 02-AUD-02-06). This report is a byproduct of the independent evaluation required by the Security Act.

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.

In its response dated December 9, 2002, the Office of Managing Director (OMD) indicated concurrence with each with each of the findings and recommendations. 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.

Walker

H. Walker Feaster III

Attachment

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

Federal Communications Commission
Office of Inspector General

FY2002 Government Information Security Reform Act Evaluation – Findings and Recommendations

Report No. 02-AUD-02-06
January 6, 2003

TABLE OF CONTENTS

Executive Summary

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

A key provision of the Security Act requires that, beginning in Fiscal Year (FY) 2001, agency Offices of Inspector General (OIG), or independent evaluators, perform an annual evaluation of the agency's information security program and practices. The OIG engaged KPMG, LLP to conduct the FY 2002 independent evaluation of the FCC's information security program and practices.

The purpose of the evaluation was to review the Commission's security program including, but not limited to, security policies, security architecture, business continuity, security capital planning, critical infrastructure, and security program planning and management. Our objective was to evaluate the effectiveness of the Commission's information security program by assessing the risk for each component of the program. Audit fieldwork began on May 17, 2002 and concluded on September 15, 2002 and was performed at FCC Headquarters, Washington, DC.

Our methodology was based upon the National Institute of Standards and Technology's (NIST) "Self-Assessment Guide for Information Technology Systems (Self-Assessment Guide)". Additional guidance was received from other NIST publications, the methodology provided in the "Federal Information Systems Control Audit Manual (FISCAM)," Federal Information Processing Standards (FIPS) publications, and other laws and directives pertaining to the protection of Federal information resources.

On September 16, 2002, we issued a report, entitled "FY 2002 Government Information Security Reform Act (GISRA) 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 information technology assets. On September 16, 2002, 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).

During the independent evaluation, we identified areas for improvement in the FCC's information security management, operational and technical controls. Specifically, we identified eight (8) findings in the areas of management, operational, and technical controls. Additionally, we determined that eight (8) of the conditions identified during the FY 2001 GISRA evaluation had not been fully corrected at the time of audit fieldwork.

Prior to issuing this report, we met with FCC management and staff about the facts comprising the conditions identified in this report. A summary of the preliminary findings was presented to FCC management at the Key Milestone Meeting on July 1, 2002. In response, FCC management provided informal written comments on July 30, 2002, which were reviewed and considered during the preparation of this report. Subsequent to the close of audit fieldwork, a preliminary draft of the Appendix B, Detailed Findings and Recommendations was forwarded to FCC Management on September 26, 2002 for additional review and comment.

On November 4, 2002, we issued a draft report summarizing the results of our audit. In that draft document, we requested that the Office of the Managing Director (OMD) respond to the findings and recommendations presented in our report. In its response dated December 9, 2002, OMD indicated concurrence with each with each of the findings and recommendations. 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.

Background

On October 30, 2000, the President signed into law the FY 2001 Defense Authorization Act (P.L. 106-398) including Title X, subtitle G, "Government Information Security Reform Act" (GISRA). GISRA amended the Paperwork Reduction Act (PRA) of 1995 by adding a new subchapter on "Information Security" and applies to all Federal Agencies. The effective date of GISRA was November 30, 2000.

A key provision of GISRA requires agency Offices of Inspector General perform an annual evaluation of the agency's information security program. GISRA also permits the OIG to select an independent evaluator to perform this evaluation. KPMG, LLP was engaged to perform the fiscal year (FY) 2002 independent evaluation.

The "Self-Assessment Guide for Information Technology Systems (Self-Assessment Guide)" issued by the National Institute of Standards and Technology (NIST) provided the framework for our methodology. As appropriate, we followed guidance prescribed by the "Federal Information Security Control Audit Manual (FISCAM)." We obtained additional guidance from other NIST publications, Federal Information Processing Standards (FIPS) publications, as well as other laws and directives pertaining to the protection of Federal information resources as listed below:

- 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, including Appendix III, "Security of Federal Automated Information Resources."
- OMB Circular A-123, entitled "Management Accountability and Control."
- OMB Circular A-127, entitled "Financial Management Systems"
- OMB M-01-08, entitled "Guidance on Implementing the Government Information Security Reform Act," dated January 16, 2001.
- OMB M-01-24, entitled "Reporting on the Government Information Security Reform Act," dated June 22, 2001.
- OMB M-02-09, entitled "Reporting Instructions for the Government Information Security Reform Act and Updated Guidance on Security Plans of Action" dated July 2, 2002.
- OMB M-97-02, entitled "Funding Information Systems Investments."
- OMB M-97-16, entitled "Information Technology Architectures."
- Federal Emergency Management Agency's Federal Preparedness Circular 65, "Federal Executive Branch Continuity of Operations (COOP)".
- The Computer Security Act of 1987 (PL 100-235).
- NIST 800-3, entitled "Establishing a Computer Security Incident Response Capability (CSIRC)."
- NIST 800-5, entitled "Guide to the Selection of Anti-Virus Tools and Techniques."
- NIST 800-12, entitled "An Introduction to Computer Security, The NIST Handbook."
- NIST Publication 800-13, entitled "Telecommunications Security Guidelines for Telecommunications Management Network."
- NIST 800-14, entitled "Generally Accepted Principles and Practices for Securing IT Systems".
- NIST 800-18, entitled "Guide for Developing Security Plans for IT Systems."
- FIPS Publication 73, entitled "Guidelines for Security of Computer Applications."
- FIPS Publication 112, entitled "Password Usage."
- FCC Instruction 1479.2, "Computer Security Program Directive."

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

<u>Objective</u>

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 this review were as follows:

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

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

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

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

5. Follow-up on the findings of the Fiscal Year 2001 GISRA review that are documented in OIG report number, 01-AUD-11-43.

Scope

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

The FY 2002 independent evaluation encompassed a review of the Commission's security program including, but not limited to, security policies, security architecture, business continuity, security capital planning, critical infrastructure, and security program planning and management.

The Security Act also requires that the OIG select an appropriate subset of agency applications for review. Our audits of the Automated Auction System and follow-up audit of computer control conditions at the FCC's Consumer Center, performed earlier in the fiscal year, satisfied this requirement. The reports on the results of these audits were issued separately and can be found in OIG Reports 02-AUD-02-08, entitled "Report on Audit of the Automated Auction System," and 01-AUD-07-30, entitled "Report on Follow-up Audit on Computer Controls at the FCC Consumer Center," respectively.

Our observations from the independent evaluation 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

Operation 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.

Observations

During our independent evaluation we reviewed documentation provided by the Commission, reviewed previously performed special reviews and audits, conducted interviews of Agency staff, and performed other activities of inquiry and observation. Audit fieldwork began on May 17, 2002 and concluded on September 15, 2002 and was performed at FCC Headquarters, Washington, DC.

As a result of observations from the evaluation, we have concluded that the Federal Communications Commission is dedicated to implementing and maintaining effective security controls aimed at protecting its information resources. Our independent evaluation for the current fiscal year yielded several positive observations relative to the Commission's information security program and practices. Positive observations included the following:

- FCC management has developed and implemented plans of action and milestones (POA&M) for each of the FY 2001 GISRA findings. Several of the prior year findings were determined to be fully remediated.

- The FCC's IT Strategic Plan was published in final format in July of 2002. The plan outlines near and long-term directions for the agency's IT architecture and program and sets forth goals reflecting the core mission and values of the IT program.

- In accordance with OMB Circular A-130, system security plans were developed for sixteen (16) of the Commission's seventeen (17) major applications and general support systems. Rules of Behavior for application users were also developed and incorporated into each of the security plans.

- A Computer Security Strategic Plan is under development. The plan is intended to address management, operational, and technical controls, physical protection of information resources, and future computer security needs of the Commission.

- The Computer Security Office has established the Computer Security Program repository on the Commission's Intranet where FCC policies, procedures, bulletins, and alerts on protecting agency's computer resources are easily accessible to authorized users of the FCC's information systems.

Since the prior year GISRA evaluation, the Commission has developed and published numerous Computer Security Desk Reference Guides that provide technical procedures for system administrators and developers for implementing the information security program and practices. Also, existing policies and procedures, such as the FCC Computer Security Directive, FCCINST 1479.2, have been updated as corrective measures to address findings reported by the FY 2001 independent evaluation. While this is noted as a positive measure, we recommend that FCC management ensure that staff and contractors responsible for implementing all new and updated policies, procedures, and guidelines are made aware of requirements. Where applicable, documentation of adherence with 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, eight (8) new findings resulted from the current year's independent evaluation. The findings consist of three (3) findings related to management controls, one (1) related to operations controls, and four (4) related to technical controls. Of the eight findings, three (3) were assigned a risk rating of 'High,' four (4) were designated with a risk level of 'Medium,' and one (1) was designated as low risk[1]. Additionally, from our follow-up on FY 2001 GISRA observations, we determined that corrective actions have not been fully implemented for eight (8) of the prior year findings.

Appendix A provides the Summary of Findings from the independent evaluation. Included as Appendix B is the report of Detailed Findings and Recommendations, provides detailed information on the conditions identified, criteria used to evaluate the condition, effect, and recommendation(s). As prescribed by OMB M-02-09, "Reporting Instructions for the Government Information Security Reform Act and Updated Guidance on Security Plans of Action", a plan of action for each finding identified during the FY 2002 independent evaluation, including milestones and completion dates, should be developed by FCC management. The plans should identify the corrective actions that the Commission intends to take to address control areas that need strengthening and identify any obstacles which may impede correction of deficiencies noted. Appendix B also lists the conditions from the FY 2001 GISRA evaluation, which were determined to have an open status from follow-up review work.

On November 4, 2002, we issued a draft report summarizing the results of our audit. In that draft document, we requested that the Office of the Managing Director (OMD) respond to the findings and recommendations presented in our report.

In its response dated December 9, 2002, OMD indicated concurrence with each with each of the findings and recommendations. 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

[1] Each finding was evaluated to determine its degree of exposure based on the following risk ratings. **High:** Security risk can cause a business disruption, if exploited. **Medium:** Security risk in conjunction with other events can cause a business disruption, if exploited. **Low:** Security risk may cause operational annoyances, if exploited.

safeguarding the non-public information contained in this report as outlined in FCCINST 1139.