OFFICE OF INSPECTOR GENERAL

MEMORANDUM

DATE: November 24, 2003

TO: Chairman

FROM: Inspector General

SUBJECT: Report on Audit of the Revenue Accounting and Management Information System (RAMIS) System.

The Office of Inspector General (OIG) has completed an Audit of the Revenue Accounting and Management Information System (RAMIS). A copy of our Audit Report, entitled "FY 2003 Audit of Revenue Accounting and Management Information System (RAMIS) application Controls," (Audit Report No. 03-AUD-01-01), is attached for your review and comment. The objective of this audit was to determine the extent and effectiveness of both application controls and general controls for RAMIS.

To accomplish the objectives of this audit, we contracted with the public accounting firm of KPMG, LLP (KPMG). Under our supervision, KPMG developed an audit plan that was designed to measure the extent that RAMIS fulfilled the above mentioned objective. This included an assessment of the current security posture of RAMIS and the use of audit tests and techniques designed to identify vulnerabilities in RAMIS controls. KPMG interviewed FCC personnel responsible for RAMIS application security, including the systems operation personnel and the Office of Managing Director (OMD) staff responsible for application development. KPMG conducted a review of technical controls on the RAMIS database to identify internal and external vulnerabilities that may lead to database compromise. For application controls, KPMG assessed authorization, completeness, accuracy, and integrity controls. The general controls review consisted of an evaluation of the major categories such as: the risk assessment process, access controls, system software, service continuity, security program planning and management, and application change controls. Finally, the review of technical controls included a vulnerability assessment that consisted of internal and external penetration testing. In addition, we reviewed the use of Auctions funding for RAMIS.

The audit yielded several positive observations about RAMIS. These included: (1) the encryption of the application's passwords; (2) improved security of the RAMIS production and

test servers; and, (3) the use of strong root passwords on the RAMIS production server and associated workstation.

We also identified areas of improvement for the FCC's security controls over RAMIS. Specifically, we identified twenty-two (22) findings in the areas of management, operational, and technical controls. Eight (8) of the twenty-two (22) findings are assigned a risk rating of 'High,' eleven (11) are assigned a rating of 'Medium,' and three (3) are assigned a rating of 'Low.' Our recommendations will correct present problems and minimize the risk that future security problems will occur in the RAMIS application. All recommendations contained in the report will be tracked for reporting purposes by the OIG.

During the audit, management proposed a revised Auctions funding percentage for RAMIS. Based on our review, we believe that the proposed funding adjustment takes into consideration the non-auction benefits of RAMIS to the Commission.

Appendix A of the attached report is a summary of the audit findings and Appendix B contains the detailed results of our audit. In addition, Appendix B contains detailed information about the methodology used, specific conditions identified, and other sensitive material collected during the review. Because of the sensitive nature of the information contained in these appendices to this report, we have classified both as Non-Public – For Internal FCC Use Only" and have limited distribution. Those persons receiving this report are requested not to photocopy or otherwise distribute this material.

In a response dated October 30, 2003, OMD indicated concurrence with the recommendations made for all fourteen findings. We have included a copy of the response from WTB in its entirety as Appendix C to this report. For twenty (20) of the twenty-two (22) findings, OMD outlined the corrective action taken and/or a milestone schedule for implementation of corrective action. For two findings, TC-6 and TC-11, OMD stated a business necessity for the condition or that compensating controls have been instituted to alleviate the condition. To explain our position on these two findings, we have added a section titled "OIG Comments," as Appendix D to this report.

Walker

H. Walker Feaster III
Inspector General

Attachment

cc: Managing Director
AMD-PERM

Federal Communications Commission
Office of Inspector General

FY2003 Audit of Revenue Accounting & Management Information System (RAMIS) Application Controls

Report No. 03-AUD-01-01
November 24, 2003

TABLE OF CONTENTS

Executive Summary

The Federal Communications Commission's (FCC or Commission) Revenue Accounting and Management Information System (RAMIS) is a mission critical information system responsible for the processing of all FCC receivable transactions. As the Commission's internal revenue management system, RAMIS supports application and regulatory fee accounting, spectrum auction loan portfolio management, accounting for auction proceeds, accounting for enforcement actions, and other accounts receivable. Once fully implemented it shall replace various independent financial management systems, including the Commission's legacy Collections system.

Factors including the high visibility of RAMIS processes, criticality of functions, and its use as a system of record for revenue accounting warranted the FCC's Office of Inspector General's (OIG) determination that an audit of RAMIS application and security controls be performed. These factors make it imperative that RAMIS be secured against internal and external computer security threats.

KPMG, LLP was engaged to perform an independent audit of the application and security controls over RAMIS. Audit fieldwork was conducted at the FCC's Portals facility in Washington, D.C., KPMG's lab in Washington, D.C., and Digital Systems Group's (DSG) Warminster, Pennsylvania headquarters during the period of March 18, 2003 through July 11, 2003.

The scope of this audit included the security infrastructure managed by the Office of Managing Director's (OMD) Information Technology Center (ITC) as it pertained to RAMIS and its related network components. Our audit approach consisted of reviewing system documentation including previous special reviews and audits, conducting interviews of FCC and DSG personnel, observing the operation of application and database security functions, and performing a vulnerability assessment of the technical controls over RAMIS.

The objective of this audit was to determine the extent and effectiveness of application and security controls of RAMIS. To achieve our objectives, we performed a review of RAMIS and its related network components using the National Institute of Standards and Technology (NIST) 800-26 Self-Assessment Guide, as well as guidance from the Federal Information System Controls Audit Manual (FISCAM). The general controls review was performed to assess controls related to the risk assessment process, access controls, system software, service continuity, security program planning, incident response, and application change controls. During the application controls review component, we evaluated authorization, completeness, and accuracy controls as well as controls over integrity of processing and data files. A review of the RAMIS database was performed to assess the security controls over critical databases, tables, and records, which included such information as payment amounts and RAMIS password controls. The final component of our audit of RAMIS application and security controls was a vulnerability assessment. The vulnerability assessment evaluated whether RAMIS and its related

network components are secure from unauthorized intrusion and misuse, vulnerable to attacks, and accessible via unauthorized paths.

Our audit yielded several positive observations about RAMIS. We also identified areas of improvement for the FCC's security controls over RAMIS. This report details the conditions identified during our audit and communicates findings and recommendations to FCC management. Specifically, we identified twenty-two (22) findings in the areas of management, operational, and technical controls. Eight (8) of the twenty-two (22) findings are assigned a risk rating of 'High', eleven (11) are assigned a rating of 'Medium', and three (3) have been designated as 'Low' risk.

Several weaknesses identified during our audit are related to controls recommended for improvement as a result of previously conducted reviews of the legacy Collections system and the RAMIS project performed under other special reviews and financial statement audits. These weaknesses are related to the lack of functional audit trails, weak user account and password management, and the lack of adequate ITC involvement in system and contractor oversight. Details of these findings, as well as all others, are listed in Appendices A and B of this report. Appendix A of the report, entitled Summary of Findings, provides a summary of the findings from this review; Appendix B, entitled Detailed Findings and Recommendations, provides detailed information on the conditions identified, criteria used to evaluate the condition, effect of the condition, and recommendation(s) for corrective actions.

The project to design and implement RAMIS has been fully funded by the Auctions program since its inception. FCC appropriated funds have not been used to support costs associated with the system. The decision to fund RAMIS with Auctions funds was in large part due to the anticipated use of the system's loan module to manage the FCC's loan portfolio. FCC management has reported that the RAMIS loan module will be removed from production when the Commission's loan service provider assumes full servicing responsibilities of the Auctions loan portfolio. As such, we recommend that FCC management finalize its re-assessment and adjustment of RAMIS funding received from the Auctions program.

On May 27, 2003, we presented preliminary findings to FCC management and DSG contractors to obtain clarification upon the facts of conditions related to general and application controls that were identified during fieldwork. Subsequent meetings were also held to ensure the validity of technical controls conditions identified during the vulnerability assessment, including identification of compensating controls.

Because of 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 Communications Commission's (FCC) Revenue Accounting and Management Information System (RAMIS) is a mission critical information system responsible for the processing of all FCC receivable transactions. As the Commission's internal revenue management system, RAMIS supports application and regulatory fee accounting, spectrum auction loan portfolio management, accounting for auction proceeds, accounting for enforcement actions, and other accounts receivable.

In accordance with Appendix III of the Office of Management and Budget (OMB) Circular A-130, RAMIS meets the criteria for a major application. As such, special management attention to the system's security is required due to the risk and magnitude of harm resulting from the loss, misuse or unauthorized access to or modification of the information in the application. The information contained in RAMIS is considered sensitive and is ranked high in its need for confidentiality, integrity, and availability.

The FCC's Financial Operations (FO) division is responsible for the development, operations, and maintenance of RAMIS. FO also oversees support services provided by RAMIS contracted personnel and FCC employees.

In FY1999, the FCC contracted Digital Systems Group (DSG) to design and implement RAMIS. RAMIS is a customized version of the accounts receivable module of DSG's Integrated Financial Management Information System (IFMIS). IFMIS is a commercial-off-the-shelf (COTS) application that has been certified as compliant with requirements of the Joint Financial Management Improvement Plan (JFMIP).

There are eight (8) modules that compose RAMIS: Loans, Fines & Forfeitures, Fees Processing, Miscellaneous Accounts Receivable, Auction Processing, International Telecommunication Settlement, Waivers & Exemptions, and Cashiering & Cash Management. Implementation of the last two (2) modules (Waivers & Exemptions and Cashiering & Cash Management) is projected for October 2003. Once fully implemented, RAMIS will replace the Commission's legacy Collections System, as well as various other independent financial management systems. The system will maintain the subsidiary journal(s) for all revenue transactions that are input into the Federal Financial System (FFS), the FCC's core accounting financial system. FCC management also plans to cease use of the Loan module, which has been implemented, after the selected service provider assumes full duties for managing the loan portfolio.

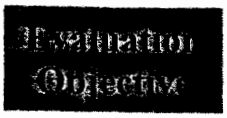
Factors including the high visibility of RAMIS processes, criticality of functions, and its function as a system of record for revenue accounting warranted the FCC's Office of Inspector General's (OIG) determination that an audit of RAMIS application and security controls be performed. These factors make it imperative that RAMIS be secured against external and internal security threats.

The guidelines for performing this audit were the Federal Information System Controls Audit Manual (FISCAM) and the National Institute of Standards and Technology (NIST)

Special Publication 800-26, "Security Self Assessment Guide for Information Technology Systems" (NIST Self Assessment Guide). Guidance was also received from additional NIST publications, as well as other laws and directives pertaining to the protection of Federal information resources. Other guidelines that were used included the following:

- 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 Circular A-130, Appendix III, "Security of Federal Automated Information Resources"
- FCC Instruction 1479.2, "FCC Computer Security Program"
- Various Other Applicable NIST Special Publications
- FCC Systems Development Life Cycle Methodology

Our procedures were designed to comply with applicable auditing standards and guidelines, specifically the Generally Accepted Government Auditing Standards (GAGAS) and American Institute of Certified Public Accountants' (AICPA) Professional Standards.



The objective of this audit was to determine the extent and effectiveness of application and security controls over the RAMIS application. The specific objectives of this audit were as follows:

1. Obtain an understanding of the Commission's RAMIS application infrastructure.

2. Obtain an understanding of the Commission's information security program and practices, particularly as it related to financial management systems and RAMIS.

3. Use application assessment methodologies, such as FISCAM or the NIST Self Assessment Guide to evaluate the effectiveness of the information security controls over RAMIS. The evaluation also included internal and external penetration tests of the network(s), operating system(s), and the RAMIS database.

4. Prepare a detailed report that will (1) identify and rank the critical RAMIS application and security control deficiencies, if any, and (2) contain observations and recommendations for improvements, if any.

During the course of the audit, the task order was modified to include a review of the development and implementation of the RAMIS loan module and assess the effectiveness of project management practices. The associated tasks were to:

1. Compile total costs associated with the loan module development and implementation.

2. Document factors that have resulted in FCC management's decision not to use the loan module for loan processing.

3. Use the information compiled in items (1) and (2) to determine if a different Auctions funding allocation method should be used for RAMIS.

4. Provide recommendations, if any, for improvements in project management and information technology (IT) capital planning practices as it relates to the RAMIS loan module.

The audit included a review of general controls related to the risk assessment process, access controls, system software, service continuity, security program planning, incident response, and application change controls. During the application controls review component we evaluated authorization, completeness, and accuracy controls as well as controls over integrity of processing and data files. A review of the RAMIS database was performed to assess the security controls over critical databases, tables, and records, which included such information as payment amounts and RAMIS password controls.

The final component of our audit of RAMIS application and security controls was a vulnerability assessment. The vulnerability assessment was conducted to evaluate whether RAMIS and its related network components are secure from unauthorized intrusion and misuse, vulnerable to attacks, and accessible via unauthorized paths. We attempted to penetrate the Commission's infrastructure at four levels by simulating external and internal security testing scenarios. The four user perspectives assumed to conduct testing were as follows:

1. An outsider with limited knowledge about FCC's IT environment;
2. An outside hacker who attacks modem connections without knowledge of the IT environment;
3. An insider with physical access to the site but with limited knowledge about FCC's IT environment; and
4. An insider with physical assess to the site and with knowledge about the IT environment.

While on the internal network, our vulnerability assessment testing was comprised of port scanning, user enumeration, vulnerability scanning, and performance of other techniques to detect possible exploitable weaknesses. The external assessment consisted of limited, high-level scanning of the FCC network.

The audit also included a task to review the effectiveness of project management and IT capital planning investment practices used to implement the RAMIS loan module. To accomplish this task we interviewed management personnel in FO to obtain information

on the design, implementation, and functionality of the RAMIS loan module. We compiled the costs of loan module enhancements using available financial data received from FO. Finally, we interviewed personnel from the Budget Office and obtained documentation of the next fiscal year's proposed RAMIS funding allocation.

Evaluation Scope

The scope of this audit included the security infrastructure managed by ITC as it pertained to RAMIS and its related network components. Our audit approach consisted of reviewing system documentation including previous special reviews and audits, conducting interviews of FCC and DSG personnel, observing the operation of application and database security functions, and performing a vulnerability assessment of the technical controls over RAMIS. Audit fieldwork was conducted at the FCC's Portals facility in Washington, D.C., KPMG's lab in Washington, DC, and DSG's Warminster, Pennsylvania headquarters from March 18, 2003 through July 11, 2003.

The observations from our audit are organized according to control areas of management controls, operational controls, and technical controls. Within each control area, specific control objectives are addressed.

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 are:

- Risk Management
- Review of Security Controls
- Life Cycle
- Authorize Processing (Certification and Accreditation)
- System Security Plan

Operational Controls - The 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 are:

- Personnel Security
- Physical Security
- Production Input/Output Controls
- Contingency Planning
- Hardware and Systems 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 control objectives addressed are:

- Identification and Authentication
- Audit Trails
- Logical Access Controls

Observation During the audit we noted several positive observations relative to RAMIS application and security controls, including the following:

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

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

- RAMIS passwords are being encrypted.

- Strong root passwords are being used on the RAMIS production server and IRIS workstation.

While the Commission has implemented numerous positive controls over RAMIS, we identified twenty-two (22) findings that impact the effectiveness of the security and control of the application. The findings consist of three (3) findings related to management controls, seven (7) related to operational controls, and twelve (12) related to technical controls. Eight (8) of the twenty-two (22) findings were assigned a risk rating of 'High', eleven (11) were assigned a rating of 'Medium', and three (3) were designated as 'Low' risk.

Several weaknesses identified during our audit are related to controls recommended for improvement as a result of previously conducted reviews of the legacy Collections system and RAMIS project performed under other special reviews and financial statement audits. These weaknesses are related to the lack of functional audit trails, weak user account and password management, and the lack of adequate ITC involvement in system and contractor oversight. The risks associated with the aggregate of weaknesses identified in these areas are summarized below:

- Non-Functional Audit Trails
  Deficiencies in audit trails increase the risk that unauthorized access to RAMIS may go undetected. As a result, critical system data pertaining to individual user accountability, reconstruction of system events, unauthorized intrusion, and problem identification may be permanently lost.

- User Accounts and Passwords
  The multiple weaknesses related to system access administered by way of user account and password management, when combined with weaknesses present in audit trails, could allow all 2,582 FCC employees and contractors unlimited access to RAMIS data files. These 2,582 "insiders" could potentially alter sensitive financial files, such as fee payments and forfeitures, without being detected. Such alterations could occur unintentionally or with malicious intent by internal users with some degree of knowledge of RAMIS.

- Segregation and Oversight of Contractor Duties
  Similar to the Report on the Federal Communications Commission's FY2001 Financial Statements (Audit Report No. 01-AUD-07-28)[1], we noted a lack of adequate ITC involvement in RAMIS system development and maintenance activities. DSG contractors have significant, unfettered control of the RAMIS application. Roles performed by DSG include application development; all aspects of change management; application, database, and operating system monitoring; system and database security administration; and user account implementation functions. Performance of these multiple system development, maintenance, and administration roles results in a notable lack of a segregation of duties.

  FO is tasked with overseeing DSG's activities and the development and operation of RAMIS. ITC's involvement in overseeing system development and maintenance activities performed by the contractor has been limited to one FCC contractor assigned to work in conjunction with DSG. However, it appears that this contractor's duties are subject to the approval of DSG. Logs generated from DSG activities are subject only to internal DSG review and are not routinely monitored by FCC personnel in FO or ITC. The end result is an increased level of unfamiliarity of the system by the FCC, particularly ITC who ensures the security of FCC major applications such as RAMIS.

The project to design and implement RAMIS has been fully funded by the Auctions program since its inception. FCC appropriated funds have not been used to support costs associated with the system. The decision to fund RAMIS with Auctions funds was in large part due to the anticipated use of the system's loan module to manage the FCC's

[1] Report on the Federal Communications Commission's FY2001 Financial Statements (Audit Report No. 01-AUD-07-28), dated April 30, 2002, page 43

loan portfolio. FCC management has reported that the RAMIS loan module shall be removed from production when the Commission's loan service provider assumes full servicing responsibilities of the Auctions loan portfolio. During interviews with personnel, we identified the need to review the Auction's funding percentage. As such, we recommend that FCC management re-assess and appropriately adjust RAMIS funding obtained from the Auctions program. The FCC's Budget Office has reported that management has begun to take steps to adjust funding and has proposed that RAMIS be funded as follows for the next fiscal year:

- 50% from Auction program funds;
- 25% from appropriated funds; and
- 25% from Credit Reform Program Act funds.

We believe that the proposed funding adjustment takes into consideration the non-Auctions related benefits to the Commission.

Appendix A of the report, entitled Summary of Findings, provides a summary of the findings from this review; Appendix B, entitled Detailed Findings and Recommendations, provides detailed information on the conditions identified, criteria used to evaluate the condition, effect of the condition, and recommendation(s) for corrective actions. As prescribed by the Federal Information Security Reform Act (FISMA) enacted by the FY2003 E-Government Act, a plan of action with associated milestones should be developed for each finding resulting from the audit. The plans should identify the corrective actions to be taken and identify any obstacles that may impede correction of deficiencies noted.

Prior to issuance of this report, the FCC and its contractor, DSG, began to take proactive steps to address these findings. We recommend that the deficiencies identified be fully corrected to strengthen the security of the RAMIS application and data. Our recommendations and those actions already begun should result in the correction of present vulnerabilities and minimization of the risk of occurrence of future security-related events.

In a response dated October 30, 2003, OMD indicated concurrence with the recommendations made for all fourteen findings. We have included a copy of the response from WTB in its entirety as Appendix C to this report. For twenty (20) of the twenty-two (22) findings, OMD outlined the corrective action taken and/or a milestone schedule for implementation of corrective action. For two findings, TC-6 and TC-11, OMD stated a business necessity for the condition or that compensating controls have been instituted to alleviate the condition. To explain our position on these two findings, we have added a section titled "OIG Comments," as Appendix D 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.