OFFICE OF INSPECTOR GENERAL

M E M O R A N D U M

DATE: January 10, 2003

TO: Chairman

FROM: Inspector General

SUBJECT: Report on the Follow-up Audit of Computer Controls at the FCC Consumer Center

The Office of Inspector General (OIG) has completed a Follow-up Audit of Computer Controls at the FCC Consumer Center. A copy of our report, entitled "Follow-up Audit on Computer Controls at the FCC Consumer Center" (Audit Report No. 01-AUD-07-30), is attached. The objective of this audit was to determine the current status of conditions identified in Audit Report No. 00-AUD-01-12, entitled "Report on Audit of Computer Controls at the FCC Consumer Center" that was issued on June 21, 2000.

To accomplish the objectives of this follow-up audit, we contracted with the public accounting firm of KPMG, LLP (KPMG). Under our supervision, KPMG first reviewed the status of each condition as reported by FCC management. The KPMG review team conducted a site visit to the FCC Consumer Center, interviewed staff, reviewed documentation, and performed other tests deemed necessary. Finally, KPMG evaluated the status of technical controls by executing automated tools and manual tests on the Consumer Center's UNIX and NT servers, as well as the Sybase databases administered by the Consumer and Governmental Affairs Bureau (CGB) and the Information Technology Center (ITC).

Of the one hundred and three (103) findings in the original audit, sixty six (66) findings were reviewed. The remaining thirty seven (37) findings were either duplicates or were otherwise determined to be outside the scope of this audit. The follow-up audit identified twenty one (21) open findings. In addition, the follow-up audit identified four (4) new conditions. We recommend that the problems we identified be corrected to strengthen the security of the Commission's Consumer Center information technology program. Our recommendations will correct present problems and minimize the risk that future security problems will occur. All recommendations contained in the attached report will be tracked for reporting purposes by the OIG.

Appendix A of the attached report is a summary of all open audit findings and new conditions. Appendix B contains the detailed results of our audit. Appendix C lists the new conditions identified during this follow-up.

On September 30, 2002, we issued a draft report summarizing the results of our audit. In that draft report, we requested that OMD and CGB prepare a joint response to the open and new findings and recommendations presented in our report and that the response be provided by October 18, 2002. On October 18, 2002, we received a request from the Commission's computer security officer to extend the due date for the response to November 1, 2002. No additional request for extension was received. On November 27, 2002, we received a response to our draft report[1].

In their response, OMD and CGB indicated concurrence with the recommendations made for all twenty five (25) new and open findings. For seventeen (17) findings, OMD and CGB outlined the corrective action taken and/or a milestone schedule for implementation of corrective action. OMD and CGB partially concurred with eight (8) findings. We have included a copy of the response from OMD and CGB in its entirety as Appendix D to this report. Where OMD and/or CGB disagreed with the finding, or to further clarify our position, we have added a section titled "OIG Comments," to explain our position or provide additional comment.

Because of the sensitive nature of the information contained in these appendices to this report, we have classified all 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.

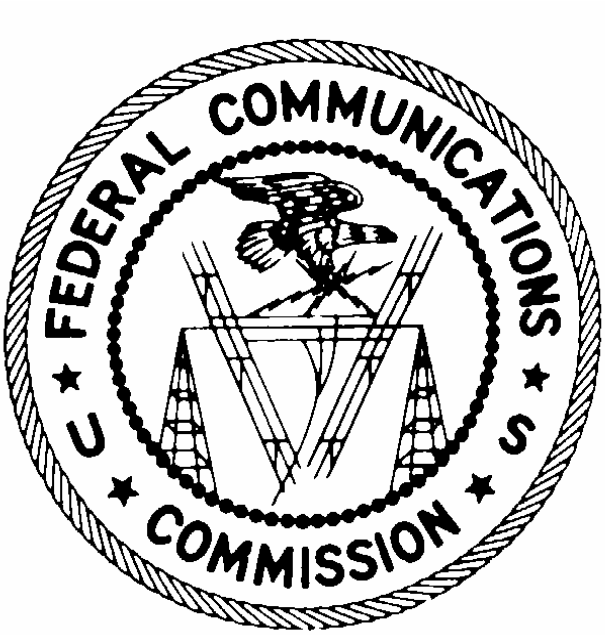
H. Walker Feaster III
Inspector General

Attachment

cc: Chief, Consumer and Governmental Affairs Bureau
Managing Director
Chief Information Officer
AMD – PERM

[1] The ITC/CGB response was dated on November 22, 2002. However, it was not provided to the OIG until November 27, 2002.

Federal Communications Commission
Office of Inspector General



Report on Follow-up Audit on Computer Controls at the FCC Consumer Center

Report No. 01-AUD-07-30
January 10, 2003

TABLE OF CONTENTS

Executive Summary

On June 21, 2000, the Office of Inspector General (OIG) issued Audit Report No. 00-AUD-01-12 entitled "Report on Audit of Computer Controls at the FCC National Call Center" summarizing the results of an audit of the FCC Consumer Center, formerly known as the National Call Center. The objective of this audit was to examine the Consumer Center's automated computer system and the environment in which it operates to ensure that adequate security safeguards exist to protect Consumer Center data.

The report noted that significant technical control and internal control improvements could be made to improve the overall security posture of the Consumer Center. The report contained one hundred three (103) specific observations and the review team concluded that the computer system general controls as implemented at the Consumer Center were not sufficient to meet minimum-security requirements. The one hundred three (103) findings covered issues in Unix, Windows NT, and Sybase controls, physical security, continuity of operations, policies and procedures, change controls, segregation of duties, and network security. The Commission concurred with all of the reported findings and developed corrective action plans to address the findings.

The OIG engaged KPMG LLP (KPMG) to perform the follow-up audit on the Consumer Center findings. The objective of this audit was to determine which findings from the audit were closed and which were open. Specifically excluded were conditions related to physical security and other conditions determined by the OIG to be outside the scope of the audit. For example, seven (7) findings dealing with slightly different aspects of UNIX file protection were combined into one finding. Also, we are planning to conduct a comprehensive physical security review in Fiscal Year 2003 which will cover the physical security issues. As a result, we are not following up on physical security findings in this review. In total, sixty-six (66) of the original one hundred three (103) conditions were followed up on during the audit. The guideline for performing this audit was the Federal Information System Control Audit Manual (FISCAM). Additional guidance was received from the National Institute of Standards and Technology (NIST) and other laws and directives related to management and protection of Federal information resources including the FCC's "Computer Security Program Directive" (FCC Instruction 1479.2).

To achieve our objective, the audit team first reviewed the status of each condition as reported by FCC management. To determine the appropriateness of the reported status and the current status of conditions, the review team conducted fieldwork from April 18, 2002 through July 23, 2002. A site visit to the FCC Consumer Center in Gettysburg, Pennsylvania was conducted on May 2, 2002 to follow up technical conditions. An additional site visit was conducted on May 6, 2002 through May 7, 2002 to review general control conditions. The remaining fieldwork was performed from the FCC's Portals location in Washington, DC. The status of general control conditions, which addressed Security Program Planning and Management, Application Software Development and Change Controls, System Software, Segregation of Duties, and Service

Continuity Service Continuity, were determined through staff interviews, review of documentation, and other tests deemed necessary. The status of technical controls conditions, which addressed Access Controls, were evaluated by executing automated tools and manual tests on the Consumer Center's UNIX and NT servers, as well as the Sybase databases administered by the Consumer and Governmental Affairs Bureau (CGB) and the Information Technology Center (ITC).

This report details our observations and documents the status of each of the conditions followed-up on. The audit also resulted in the identification of additional control weaknesses. Specifically, of the sixty-six (66) findings followed up on, twenty-one (21) were determined to have an open status, forty-five (45) were identified as closed. The audit also resulted in the identification of four (4) new conditions.

On July 1, 2002, we met with representatives from the ITC, CGB, and the FCC Security Office to discuss preliminary findings. In response, ITC and CGB provided informal written comments.

On September 30, 2002, we issued a draft report summarizing the results of our audit. In that draft report, we requested that OMD and CGB prepare a joint response to the open and new findings and recommendations presented in our report and that the response be provided by October 18, 2002. On October 18, 2002, we received a request from the Commission's computer security officer to extend the due date for the response to November 1, 2002. No additional request for extension was received. On November 27, 2002, we received a response to our draft report[1].

In their response, OMD and CGB indicated concurrence with the recommendations made for all twenty five (25) new and open findings. For seventeen (17) findings, OMD and CGB outlined the corrective action taken and/or a milestone schedule for implementation of corrective action. OMD and CGB partially concurred with eight (8) findings. We have included a copy of the response from OMD and CGB in its entirety as Appendix D to this report. Where OMD and/or CGB disagreed with the finding, or to further clarify our position, we have added a section titled "OIG Comments," to explain our position or provide additional comment.

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 (FCC) Office of the Inspector General (OIG) is responsible for conducting audits and investigations of FCC operations and programs. The OIG provides leadership and recommends policies for activities designed to prevent and detect fraud, waste, and abuse and to promote economy, efficiency, and effectiveness

[1] The ITC/CGB response was dated on November 22, 2002. However, it was not provided to the OIG until November 27, 2002.

of FCC programs and operations. Since its creation in 1988, the OIG has performed numerous reviews, inspections, and audits to evaluate the effectiveness of controls designed to ensure the protection of Commission personnel and property. For example, the OIG has performed several reviews evaluating the security of the Commission's Information Technology (IT) infrastructure (e.g., security of network components, data centers, hub rooms, wiring closets, etc.) and several reviews to evaluate the physical security of Commission workspace.

On June 21, 2000, the OIG issued Audit Report No. 00-AUD-01-12 entitled "Report on Audit of Computer Controls at the FCC National Call Center" summarizing the results of our audit of the FCC Consumer Center, formerly known as the National Call Center. The objective of this audit was to examine the Consumer Center's automated computer system and the environment in which it operates to ensure that adequate security safeguards exist to protect Consumer Center data.

The report noted that significant technical control and internal control improvements could be made to improve the overall security posture of the Consumer Center. The original report contained one hundred three (103) specific observations in the area of internal controls including: Security Program Planning and Management, Access Controls, Application Software Development and Change Controls, System Software, Segregation of Duties, and Service Continuity. Accordingly, the review team concluded that the computer system general controls as implemented at the Consumer Center were not sufficient to meet minimum-security requirements

The one hundred three (103) findings covered issues related to Unix, Windows NT, and Sybase controls, physical security, continuity of operations, policies and procedures, change controls, segregation of duties, and network security. Thirteen (13) were classified with a high level of risk, fifty-two (52) with a medium level of risk, and thirty-eight (38) with a low level of risk. The Commission concurred with all of the reported findings and developed corrective action plans to address the findings.

The guideline for performing this audit was the Federal Information System Control Audit Manual (FISCAM). Additional guidance was received from the National Institute of Standards and Technology (NIST) and the following laws and directives related to management and protection of Federal information resources:

- 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."
- The Computer Security Act of 1987 (PL 100-235).
- FCC Instruction 1479.2, "Computer Security Program Directive."

Objective

The purpose of this audit was to determine the current status of the conditions at the FCC Consumer Center identified in Audit Report No. 00-AUD-01-12, entitled "Report on Audit of Computer Controls at the FCC Consumer Center".

To achieve our objective, the audit team first reviewed the status of each condition as reported by FCC management. To determine the appropriateness of the reported status and the current status of conditions, the review team conducted a site visit to the FCC Consumer Center. The status of general control conditions, which addressed control areas of Security Program Planning and Management, Application Software Development and Change Controls, System Software, Segregation of Duties, and Service Continuity Service Continuity, were determined through staff interviews, review of documentation, and other tests deemed necessary. The status of technical controls which addressed the control area of Access Controls were evaluated by executing automated tools and manual tests on the Consumer Center's UNIX and NT servers, as well as the Sybase databases administered by the Consumer Governmental Bureau (CGB) and the Information Technology Center (ITC).

Scope

The scope of this engagement consisted of control weaknesses identified in the OIG's prior report on the Consumer Center, Audit Report No. 00-AUD-01-12, Report on Audit of Computer Controls at the FCC National Call Center, issued June 21, 2000. The scope of this task order was to determine which findings from the prior audit were closed or open. For closed findings, the contractor performed appropriate tests to determine if the closed status was appropriate. For findings reported as open, the contractor determined if the condition still existed and if the open status was still appropriate. Our procedures were designed to comply with applicable auditing standards and guidelines, specifically the Generally Accepted Government Auditing Standards (GAGAS).

The review team conducted fieldwork from April 18, 2002 through July 23, 2002. A site visit to the FCC Consumer Center in Gettysburg, Pennsylvania was conducted on May 2, 2002 to follow up technical conditions. An additional site visit was conducted on May 6, 2002 through May 7, 2002 to review general control conditions. The remaining fieldwork was performed from the FCC's Portals location in Washington, DC.

Specifically excluded from this audit were conditions related to physical security, conditions determined to affect the FCC as a whole and other conditions which did not warrant follow-up as, determined by the OIG. In total, sixty-six (66) of the one hundred three (103) conditions were reviewed and thirty-seven (37) were excluded. Our objective was to determine the appropriateness of the status of conditions reported by FCC management and determine which findings from the audit were closed and which were open.

Observations

The FCC Consumer Center findings identified during the original audit of computer controls covered issues in Unix, Windows NT, and Sybase controls, physical security, continuity of operations, policies and procedures, change controls, segregation of duties, and network security.

Included in our follow-up audit were sixty-six (66) of the one hundred three (103) FCC Consumer Center conditions identified in Audit Report No. 00-AUD-01-12. FCC management had reported sixty-four (64) of the sixty-six (66) conditions as resolved through corrective actions taken subsequent to issuance of Audit Report No. 00-AUD-01-12. Two (2) conditions were reported as unresolved and thus open at the time that our audit commenced.

Of the sixty-six (66) conditions that were reviewed, the audit identified twenty-one (21) conditions with an 'open' status, forty-five (45) with a 'closed' status, and four (4) new control weaknesses. Represented in the open conditions are twenty (20) that were determined to exist in the Consumer Center environment at the time of our audit which had been reported as resolved by FCC management prior to the audit. As a result, these conditions have been re-opened. From our review, we were able to ascertain that some of these conditions may have re-opened for reasons including the degradation of security controls after the initial corrective action was taken, introduction of new hardware which may not have been properly configured, or subsequent changes made by personnel with administrative and maintenance duties.

Of those conditions determined to have an open status, five (5) were classified as having high levels of risk, thirteen (13) as medium levels of risk, and three (3) as low risk levels in the original audit. Of the new control weaknesses identified during the audit, two (2) have been determined to have high levels of risk and the remaining two (2) a medium level of risk.

During the review, FCC management took proactive measures to investigate the conditions identified as open and initiated steps to resolve those conditions. As applicable, we have noted such activities of corrective actions in our report.

Appendix A of this report provides the FCC Consumer Center Audit - Findings Summary which lists all open and new conditions identified during fieldwork. Appendix B of the report, entitled FCC Consumer Center Audit - Detailed Findings, provides detailed information on the conditions identified during fieldwork. Additional fields to indicate (1) the status of conditions as reported by FCC management prior to the audit, (2) observations from the follow-up audit, and (3) the status of the conditions as determined by the auditor were added to the Detailed Findings report provided in Audit Report No. 00-AUD-01-12. The report also indicates corrective actions reported to have been taken during our audit by FCC management to resolve conditions determined to have an open status. The report entitled FCC Consumer Center Audit - New Conditions Identified is

included as Appendix C to document new conditions at the FCC Consumer Center identified during the follow-up audit.

On September 30, 2002, we issued a draft report summarizing the results of our audit. In that draft report, we requested that OMD and CGB prepare a joint response to the open and new findings and recommendations presented in our report and that the response be provided by October 18, 2002. On November 27, 2002, we received a response to our draft report.

In their response, OMD and CGB indicated concurrence with the recommendations made for all twenty five (25) new and open findings. For seventeen (17) findings, OMD and CGB outlined the corrective action taken and/or a milestone schedule for implementation of corrective action. OMD and CGB partially concurred with eight (8) findings. We have included a copy of the response from OMD and CGB in its entirety as Appendix D to this report. Where OMD and/or CGB disagreed with the finding or to clarify our position, we have added a section titled "OIG Comments," to explain our position or provide additional comment.

In accordance with the Commission's directive on the management of non-public information, we have classified all appendices as "Non-Public – For Internal Use Only." Those persons receiving this report are expected to follow the established policies and procedures for managing and safeguarding this report in accordance with the Commission directive.