OFFICE OF INSPECTOR GENERAL

MEMORANDUM

DATE: October 22, 2004

TO: Chairman

FROM: Inspector General

SUBJECT: Report on Follow Up to the Audit of Web Presence Security

The Office of Inspector General (OIG) has completed an Audit of Web Presence Security. A copy of our Audit Report, entitled "Follow Up to the Audit of Web Presence Security" (Audit Report No. 03-AUD-09-21) is attached for your review and comment. The objective of this audit was to determine the current status of conditions identified in Audit Report No. 00-AUD-01-10, entitled "Audit of Web Presence Security" that was issued on June 13, 2001.

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 audit team 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 devices comprising the FCC's web presence. These tests included a vulnerability assessment to test the security of the Commission's web-based assets.

During the FY 2003 follow-up audit we identified a number of positive security controls in the FCC's web presence, including:

- The use of generic and group accounts was effectively managed by the Information Technology Center (ITC)
- The Auctions Operations Branch operated a robust network security intrusion detection system (IDS)

While positive security controls were noted, the audit identified that corrective actions had not been fully implemented for all of the original audit findings. For the thirty-seven (37) findings followed up on, twenty-eight (28) were determined to have a closed status and nine (9) were identified as open. Of the nine (9) open findings, one (1) was classified as high risk. In addition, the follow-up audit disclosed five (5) new conditions. Of the five (5) new conditions, one (1)

was classified as high risk. This new high risk condition was corrected during the audit period. Appendix A, Summary of Findings, summarizes these conditions. Appendix B, Detailed Findings and Observations, contains the detailed results of our audit and contains detailed information about follow-up to the findings of the original audit. Appendix C, New Conditions, details the five (5) new conditions identified. All recommendations contained in the attached report will be tracked for reporting purposes by the OIG.

On August 31, 2004, we provided a draft report to the Office of Managing Director (OMD) and the Wireless Telecommunication Bureau (WTB) for review and comments. In a response dated September 29, 2004, OMD concurred with eight (8) of the findings. OMD indicated partial concurrence with two (2) of the findings. For four (4) of the findings, OMD stated that corrective action was taken before the end of audit fieldwork. We have included a copy of the response in its entirety as Appendix D to this report.

Because of the sensitive nature of the information contained in the appendices to this report, we have marked all appendices as "Privileged and Confidential, Non-Public – For Internal FCC Use Only" and have severally 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: Managing Director
Chief, Wireless Telecommunications Bureau
AMD-PERM

Federal Communications Commission
Office of Inspector General

FY 2003 Follow-up on the Audit of Web Presence Security

Audit Report No. 03-AUD-09-21
October 20, 2004

TABLE OF CONTENTS

EXECUTIVE SUMMARY

On June 13, 2001, the Federal Communications Commission (FCC or Commission) Office of Inspector General (OIG) issued Audit Report No. 00-AUD-01-10, Audit of Web Presence Security. The report summarized the results of the audit of the FCC's program for managing its web presence. Web presence was defined as the infrastructures developed to maintain the Commission's systems that allow the public to submit applications and/or filings via the Internet. These infrastructures, managed by the Information Technology Center (ITC) and the Auctions Automation Branch of the Wireless Telecommunications Bureau (WTB), included all hardware, software, and network services that comprised the Commission's Internet entry and egress points.

The objective of the FY 2001 audit was to measure the Commission's success at securing its web portals. The audit concluded that the FCC had an active and generally effective program for managing web presence security. The report cited several positive computer security controls. However, 38 security findings, for which corrective actions were recommended, were also identified. As of August 8, 2004, FCC management had reported on-going corrective actions for 14 of the findings. Corrective actions for the remaining 24 were reported as completed.

In FY 2003, the OIG engaged KPMG LLP to perform a follow-up audit on the status of corrective actions for findings identified by the original audit of the FCC's web presence security. The scope of the follow-up audit included the respective web presence infrastructures managed by ITC and the Auctions Operations Branch. Follow-up was conducted on 37 of the 38 original audit findings and specifically excluded devices and systems that support web services that were located at the FCC's Consumer Center in Gettysburg, PA.

The objectives of the follow-up audit were to ensure that appropriate corrective actions have been implemented and test the current security posture of the FCC's web presence. To achieve our objectives, we conducted external penetration tests of select e-filing applications, including attempts to login to e-filing applications from the Internet. The audit team also used automated tools, conducted manual tests and other techniques, and interviewed personnel to determine the status of the original audit findings. Fieldwork was conducted at the FCC's Washington, DC Portals headquarters between the period of September 24, 2003 and June 18, 2004.

The Federal Information System Controls Manual (FISCAM) provided the framework for conducting this audit. In particular, Appendix III of the FISCAM, *Tables for Summarizing Work Performed in Evaluating and Testing General Controls*, was referenced as guidance. Guidance was also obtained from additional publications issued by the National Institute of Standards and Technology (NIST), other laws and directives pertaining to the protection of Federal information resources, and Commission-specific guidance, including the FCC's "Computer Security Program Directive" (FCC Instruction 1479.2).

As in the original audit of the FCC's web presence security, we identified several positive controls during the FY 2003 follow-up fieldwork. However, the audit identified that corrective actions had not been fully implemented for all of the original audit findings. For the thirty-seven (37) findings followed up on, twenty-eight (28) were determined to have a closed status and nine

(9) were identified as open. Of the nine (9) open findings, one (1) was classified as high risk. In addition, the follow-up audit disclosed five (5) new conditions. Of the five (5) new conditions, one (1) was classified as high risk. This new high risk condition was corrected during the audit period.

As a result of our review of the status of follow-up audit findings, we specifically recommend that ITC prioritize resources to make improvements in its patch management and intrusion detection practices. These practices are a direct cause of several follow-up findings related to hardware/system software maintenance and audit trail controls. On-going weaknesses resulting from patch management and intrusion detection have been identified by several audits of FCC security controls, including the original web presence audit, and are considered to be systemic in nature.

Appendices A, B, and C to this report provide the details of follow-up observations noted during the audit, the status of corrective actions, and new security weaknesses identified during this follow-up review. Over the course of the audit, FCC management took proactive measures to investigate several findings identified as open and new and in some cases initiated steps to correct these issues. As applicable, we have noted such activities of corrective actions in our report.

Prior to issuing this report, we took steps to reach agreement with FCC management upon the facts of the conditions identified in this report. During the audit and at the audit's Exit Conference held on June 22, 2004, preliminary findings were presented to ITC and WTB's Auctions Operations Branch. The informal comments received by the audit team were considered during the preparation of this report, and incorporated as appropriate.

On August 31, 2004, we provided a draft report to the Office of Managing Director (OMD) and the Wireless Telecommunication Bureau (WTB) for review and comments. In a response dated September 29, 2004, OMD concurred with eight (8) of the findings. OMD indicated partial concurrence with two (2) of the findings. For four (4) of the findings, OMD stated that corrective action was taken before the end of audit fieldwork. OMD outlined the corrective action to be taken and a schedule for implementation of corrective action. We have included a copy of the response in its entirety 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.

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 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. The FCC's OIG has performed several reviews evaluating the security of the Commission's Information Technology (IT) infrastructure as well as the physical security of the Commission's workspace.

On June 13, 2001, the OIG issued Audit Report No. 00-AUD-01-10, Audit of Web Presence Security. The report summarized the results of the audit of the Commission's program for managing its web presence. Web presence was defined as the infrastructures developed to maintain the Commission's systems that allow the public to submit applications and/or filings via the Internet. The infrastructures, managed by the Information Technology Center (ITC) and the Auctions Automation Branch of the Wireless Telecommunications Bureau (WTB), included all hardware, software, and network services that comprised the Commission's Internet entry and egress points.

The objective of the FY 2001 audit was to measure the Commission's success at securing its web portals. The audit concluded that the FCC had an active and generally effective program for managing web presence security. The report cited several positive computer security controls that were designed to protect and preserve web-based assets. However, thirty-eight (38) security weaknesses related to host and network access, system software, service continuity, and application software development controls were also identified. Six (6) of the findings were designated as high-risk, thirty-one (31) medium-risk, and one (1) low-risk. Corrective actions were recommended for each.

Implementation of corrective actions to Commission audit findings are reported to and tracked by the FCC's Performance Evaluation and Records Management (PERM) office. As of August 8, 2003, corrective actions for fourteen (14) of the findings from the original web presence audit were reported by FCC management as on-going and twenty-four (24) as completed. ITC reported that corrective actions were in progress for several findings that pertained to the FCC HQ Public DMZ. The Auctions Automation Branch had reported that all findings affecting the WTB Auctions DMZ had been resolved.

In FY 2003, the OIG engaged KPMG LLP to perform a follow-up audit on the status of corrective actions for findings identified by the original FY 2001 web presence security audit. The Federal Information System Controls Manual (FISCAM) provided the framework for conducting this audit. In particular, Appendix III of the FISCAM, *Tables for Summarizing Work Performed in Evaluating and Testing General Controls*, was used as guidance where appropriate. Guidance was also obtained from additional publications issued by the National Institute of Standards and Technology (NIST), as well as the following laws and directives and Commission-specific guidance:

- 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
- FCC Instruction 1479.2, "Computer Security Program Directive"
- FCC Performance Evaluation & Records Management (PERM) Audit Follow-up Guidelines
- NIST Self Assessment Guide, Special Publication 800-26

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

AUDIT OBJECTIVES

The objectives of the FY 2003 follow-up audit were to: (1) follow-up on specific observations identified in Audit Report No. 00-AUD-01-10 to ensure appropriate corrective actions had been implemented; and (2) perform tests on the information systems security posture of the web presence.

To achieve the follow-up audit objectives, the audit team conducted external penetration tests of select e-filing applications, including attempts to login to e-filing applications from the Internet. The audit team also used automated tools, conducted manual tests and other techniques, and interviewed personnel to determine the status of the original audit findings and the security posture of the FCC's web presence infrastructure

SCOPE

The scope of the follow-up audit included the FCC HQ Public DMZ and WTB Auctions DMZ respectively managed by ITC and the Auctions Operations Branch. Follow up was conducted on corrective actions for thirty-seven (37) of the thirty-eight (38) original audit findings from Audit Report No. 00-AUD-01-10, Report on Web Presence Security. Specifically excluded were devices and systems supporting web services that were located at the FCC's Consumer Center in Gettysburg, PA. E-filing systems that were included in external penetration tests were the Commission's Registration System (CORES), the International Bureau Filing System (IBFS), the Consolidated Database System (CDBS), the Enforcement Bureau Filing System (EBFS), and the Electronic Tariff Filing System (ETFS). Audit fieldwork was conducted at the FCC's Washington, DC Portals headquarters between the period of September 24, 2003 and June 18, 2004.

Follow-up audit findings have been organized according to the NIST control areas of management controls, operational controls, and technical controls. The control areas are defined below and the specific control techniques addressed by each are outlined.

Management Controls – Management controls focus on the management of the IT security system and the management of risk for a system. They are techniques and concerns that are normally addressed by management. The specific management control objectives addressed

were:

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

Operational Controls – Operational controls address security methods focusing on mechanisms primarily implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise and often rely upon management activities as well as technical controls. The specific operational control objectives addressed were:

- Personnel Security
- Physical and Environmental Protection
- Production, Input/Output Controls
- Contingency Planning
- Hardware and System Software Maintenance
- Data Integrity
- Documentation
- Security Awareness, Training and Education
- Incident Response Capability

Technical Controls - Technical controls focus on security controls that the computer system executes. The controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. The specific technical operational control objectives addressed were:

- Identification and Authentication
- Audit Trails
- Logical Access Controls

New findings that resulted from the audit have 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:

<u>High Risk:</u>	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: Security risk may cause operational annoyances, if exploited.

AUDIT OBSERVATIONS

During the FY 2003 follow-up audit we identified the following positive security controls in the FCC's HQ Public DMZ, which is managed by ITC:

- Remote access to devices within the DMZ were tightly controlled;
- The use of generic and group accounts was effectively managed; and
- Administrative access was appropriately controlled and monitored through logging mechanisms.

We also identified that the WTB's Auctions Operations Branch had implemented the following positive security controls within the WTB Auctions DMZ:

- A robust intrusion detection system (IDS);
- Strong management of user accounts and passwords on hosts that were tested; and
- Appropriate control and monitoring of administrative access through logging mechanisms.

While positive security controls were noted, the audit identified that corrective actions had not been fully implemented for all of the original audit findings. For the thirty-seven (37) findings followed up on, twenty-eight (28) were determined to have a closed status and nine (9) were identified as open. Of the nine (9) open findings, one (1) was classified as high risk. These open findings are related to hardware/system software maintenance, logical access, identification and authentication, and audit trails. ITC has been noted as having sole responsibility over seven (7) of the open findings applicable to the FCC HQ Public DMZ identified by the original report. The responsibility for the eighth finding in the FCC HQ Public DMZ is shared by ITC, the Financial Systems Operations Group, and the International Bureau. The ninth finding noted as open during fieldwork was applicable to the WTB Auctions DMZ. This finding was corrected by the Auctions Operations Branch during follow-up audit fieldwork and is noted in this report as closed.

The audit identified that eight (8) of the original nine (9) audit findings determined to be open during our follow-up audit had been reported to PERM as closed by FCC management prior to

the audit. 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.

Five (5) new conditions in the areas of operational and technical controls were also identified. These findings are related to hardware/system software maintenance and logical access controls. Of the new control weaknesses identified, one (1) has been classified as high risk, two (2) as medium risk, and two (2) as low risk. This new high risk condition was corrected during the audit period.

As a result of follow-up audit findings, we specifically recommend that ITC prioritize resources to make improvements in its patch management and intrusion detection practices. Patch management and intrusion detection are among an entity's first line of defense against IT security threats and attacks. On-going weaknesses in these areas have been identified by several audits of FCC security controls, including the original web presence audit, and are considered to be systemic in nature. Patch management practices can be directly linked to several of the follow-up audit findings related to hardware/system software maintenance controls, including two (2) of the new findings. The FCC ITC's lack of strong controls surrounding the management and monitoring of the intrusion detection system is a cause of follow-up audit findings related to audit trail controls.

Over the course of the audit, FCC management took proactive measures to investigate several conditions identified as open and new. In some cases steps were initiated to fully implement corrective actions and resolve the findings noted. As applicable, we have identified these activities of corrective actions in our report.

Prior to issuing this report, we took steps to reach agreement with FCC management upon the facts of the conditions identified in this report. Over the course of the audit and at the audit's Exit Conference held on June 22, 2004, preliminary findings were presented to ITC and the Auctions Operations Branch. The informal comments received from each entity were considered during the preparation of this report, and incorporated as appropriate.

Appendix A of this report is a Summary of Findings and provides a summary of all open and new conditions identified during fieldwork. Appendix B to the report, Detailed Findings and Observations, provides detailed information on the 37 follow-up observations included in the scope of this audit and the corrective status of each as noted during fieldwork. This appendix was prepared by adding additional fields to the Detailed Findings and Recommendations report issued by Audit Report No. 00-AUD-01-10. The added fields indicate (1) the status of conditions as reported by FCC management to PERM prior to the audit, (2) observations from the follow-up audit, (3) the status of the conditions as determined by the auditor, and (4) the FCC entity responsible for open findings. Appendix C, New Conditions – Detailed Findings and Recommendations, provides the details of the new conditions identified.

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

the Wireless Telecommunication Bureau (WTB) for review and comments. In a response dated September 29, 2004, OMD concurred with eight (8) of the findings. OMD indicated partial concurrence with two (2) of the findings. For four (4) of the findings, OMD stated that corrective action was taken before the end of audit fieldwork. OMD outlined the corrective action to be taken and a schedule for implementation of corrective action. We have included a copy of the response in its entirety 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.