*OFFICE OF INSPECTOR GENERAL*

**M E M O R A N D U M**

**DATE:** June 13, 2001

**TO:** Chairman

**FROM:** Inspector General

**SUBJECT:** Report on 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 "Audit of Web Presence Security" (Audit Report No. 00-AUD-01-10), is attached for your review and comment. The objective of this audit was to measure how successful the Commission has been in securing its web portals. Because the use of the Internet for commerce presents new and unique security challenges, we developed a set of specific information security related objectives for this audit. Specific objectives were to:

- Determine if any conditions exist that could allow external user or hacker to penetrate web server security and cause possible harm to Commission assets;
- Ensure that the FCC is not vulnerable to known Web-based security attacks; and
- Identify vulnerabilities in the general controls over web-based assets.

To accomplish the objectives of this audit, we contracted with the computer security firm of TWM Associates, Inc. (TWM) to perform the audit. Under our supervision, TWM developed an audit plan that was designed to measure the extent that the Commission's web presence infrastructure fulfilled the above mentioned security goals. This audit included an assessment of the current security posture of those Commission-wide systems providing information via the Web and the use of audit tests and techniques designed to identify vulnerabilities in web presence security. We interviewed FCC personnel responsible for Internet and web security, including the Computer Security Office (CSO), Information Technology Center (ITC) and Auctions systems personnel, and Bureau and Office personnel responsible for application development. We also reviewed FCC system documentation. In addition, we performed a number of tests to determine the level of security of the FCC's web presence. For example, to determine what Internet system services the FCC web hosts offered, TWM examined the ITC and Auctions systems using a network scanning tool and used a proprietary program to perform sophisticated analyses of the FCC's Unix and Windows NT web presence hosts. Finally, we used system penetration techniques to test the security of the Commission's web-based applications.

During our audit, we found that the Commission has implemented numerous computer security controls designed to protect and preserve its web-based assets. However, during the audit, we identified thirty-eight findings (38) that impact the effectiveness of the Commission's program. Six (6) of the audit findings were determined to be high-risk[1], thirty-one (31) were determined to be medium risk, and one (1) was determined to be low risk. Findings occurred in the areas of host and network access, system software, service continuity, and application software development controls. We recommend that the problems we identified be corrected to strengthen the security of the Commission's web presence. Our recommendations, when implemented, will correct present problems and minimize the risk that future security problems will occur in the FCC's Internet web presence. All recommendations contained in the attached report will be tracked for reporting purposes by the OIG.

On March 28, 2001, we issued a draft report summarizing the results of our audit. In that draft report, we requested that the Wireless Telecommunications Bureau (WTB) and the Information Technology Center (ITC) respond to the findings and recommendations presented in our report. Each organization prepared a response addressing those findings and recommendations relevant to their portion of the Information Technology infrastructure. ITC provided comments on thirty-one (31) of the thirty-eight (38) findings contained in the draft report and WTB provided responses to twenty (20) findings.

In their response, ITC indicated concurrence with twenty-eight (28) of the thirty-one (31) findings for which they provided a response and indicated that they did not concur with three (3) findings. For one (1) of the findings with which ITC did not concur, we examined the response, agreed with ITC's explanation and closed the finding. For two (2) of the findings where ITC indicated that they did not concur, ITC explains that the finding has been addressed by events that took place after fieldwork was completed on the audit. For each of these findings, we state in our comments that ITC should demonstrate this solution as part of the audit follow-up process to close this finding. We have included a copy of the response from ITC in its entirety as Appendix D to this report. Where ITC disagreed with our conclusions, we have added a section titled "OIG Comments," to explain our position.

In their response, WTB indicated concurrence with each of the recommendations for the twenty (20) findings that applied to the bureau. Of these twenty (20) findings, WTB reported that fifteen (15) were closed as of May 7, 2001. We have included a copy of the response from WTB in its entirety as Appendix C to this report.

---

1 Each audit 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.

Because of the sensitive nature of the information contained in the appendices, we have marked them all "Privileged and Confidential, 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.

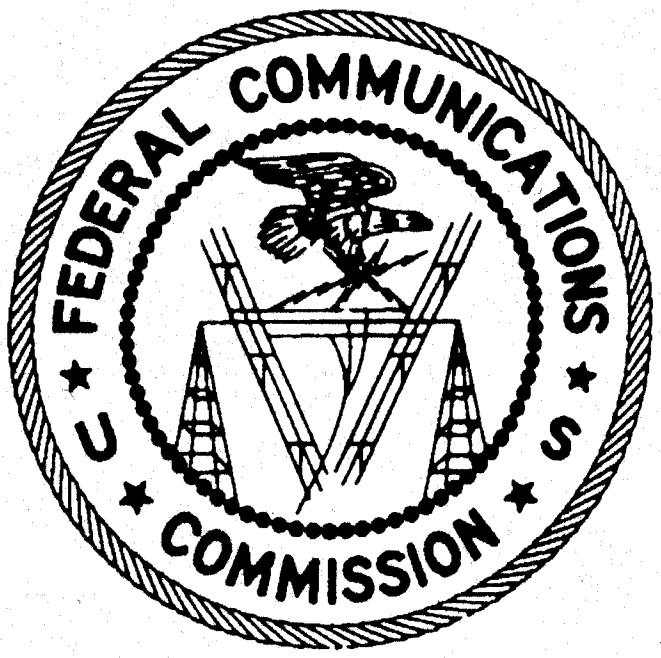
H. Walker Feaster III
Inspector General

Attachment

cc: Chief of Staff
Managing Director
Chief, Wireless Telecommunications Bureau
Chief Information Officer
AMD-PERM

# FEDERAL COMMUNICATIONS COMMISSION

## OFFICE OF INSPECTOR GENERAL




Audit of Web Presence Security

Audit Report No. 00-AUD-01-10
June 13, 2001

H. Walker Feaster III
Inspector General

Thomas D. Bennett
Assistant Inspector General – Audits

Walter P. Opaska
Director – IS Audits

# Audit of Web Presence Security

## Table of Contents

## EXECUTIVE SUMMARY

The Federal Communications Commission (FCC) is increasingly using the Internet to conduct business and to disseminate information. For example, the Commission currently maintains several internet-based electronic filing (e-filing) systems that allow the public to submit and/or review the different types of filings related to FCC proceedings, rulemakings, tariffs, and official forms. To maintain those systems that allow the public to submit and/or filings via the Internet, the FCC has developed an infrastructure that we have called the web presence. The web presence includes all hardware, software, and network services that comprise the Commission's Internet entry and egress points. We liken the Web Presence to the FCC's doors and windows on the Internet.

Just as a prudent businessperson would check the security of the office doors and windows, we developed the scope of this audit to assess the current security posture of the FCC's web presence. Again, like the businessperson, we focused much of our efforts on the external threat. Because the use of the Internet for commerce presents new and unique security challenges, we developed a set of specific information security related objectives for this audit. They include:

- Determine if any conditions exist that could allow external user or hacker to penetrate web server security and cause possible harm to Commission assets.
- Ensure that the FCC is not vulnerable to known Web-based security attacks.
- Identify vulnerabilities in the general controls over web-based assets.

To gauge the extent that the FCC met these goals, we contracted with TWM Associates, Inc. (TWM) to conduct an audit of web presence security. Under our guidance and supervision, TWM developed an audit workplan designed to measure the extent that the Commission's web presence infrastructure fulfilled the above mentioned security goals. This audit workplan served as the basis for the audit TWM conducted on the web presence. This audit included an assessment of the current security posture of those Commission-wide systems providing information via the Web and the use of audit tests and techniques designed to identify vulnerabilities in web presence security.

During our audit, we found that the Commission has implemented numerous computer security controls designed to protect and preserve its web-based assets. However, during the audit, we identified thirty-eight findings (38) that impact the effectiveness of the Commission's program. These findings occurred in the areas of host and network access, system software, service continuity, and application software development controls. We recommend that the problems we identified be corrected to strengthen the security of the Commission's web presence. Our recommendations will correct present problems and minimize the risk that future security problems will occur in the FCC's Internet web presence.

The two entities primarily responsible for the security of the FCC's Web Presence, the Wireless Telecommunications Bureau (WTB) and the Information Technology Center

(ITC), prepared separate responses to the draft report and its thirty-eight (38) findings. In the WTB response, the Chief, WTB, concurred with the with the recommendations for the twenty (20) findings that applied to the bureau. Of these twenty (20) findings, WTB reported that fifteen (15) were closed as of May 7, 2001. We have included a copy of the response from WTB in its entirety as Appendix C to this report.

In the ITC response to the draft report, the Chief Information Officer (CIO) concurred with or concurred with comments to twenty-eight (28) of the thirty-one (31) findings that applied to ITC. The ITC disagreed with the recommendations of three (3) findings. Also, ITC requested that we reclassify the severity of a third finding, while concurring with its recommendation. In response, we have added our comments to the end of these four (4) findings. We have included a copy of the response from ITC in its entirety as Appendix D to this report. Where ITC disagreed with our conclusions, we have added a section titled "OIG Comments," to explain our position.

## AUDIT OBJECTIVE

The objective of this audit was to measure how successful the Commission has been in securing its web portals. Because the use of the Internet for commerce presents new and unique security challenges, we developed a set of specific information security related objectives for this audit. Specific objectives were to:

- Determine if any conditions exist that could allow external user or hacker to penetrate web server security and cause possible harm to Commission assets.
- Ensure that the FCC is not vulnerable to known Web-based security attacks.
- Identify vulnerabilities in the general controls over web-based assets.

To gauge the extent that the FCC met these goals, we contracted with TWM to perform the audit on the web presence. Under our supervision, TWM developed an audit workplan that was designed to measure the extent that the Commission's web presence infrastructure fulfilled the above mentioned security goals. This audit workplan served as the basis for the audit TWM conducted on the web presence. This audit included an assessment of the current security posture of those Commission-wide systems providing information via the Web and the use of audit tests and techniques designed to identify vulnerabilities in web presence security.

We employed the following audit techniques to accomplish this objective. We interviewed FCC personnel responsible for Internet and web security, including the Computer Security Office (CSO), Information Technology Center (ITC) and Auctions systems personnel, and Bureau and Office personnel responsible for application development. We sent questionnaires and e-mails to the CSO, and selected Bureau and Office personnel. We also reviewed FCC system documentation.

In addition, we performed a number of tests to determine the level of security of the FCC's web presence. To determine what Internet system services the FCC web hosts offered, TWM examined the ITC and Auctions systems using nmap, a commonly used network scanning tool by auditors and computer security professionals. TWM used a proprietary program to perform sophisticated analyses of the FCC's Unix and Windows NT web presence hosts. Finally, we used system penetration techniques to test the security of the Commission's web-based applications.

## AUDIT SCOPE

This audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) and included such analyses, interviews, and testing as required to support the audit findings.

The scope of this audit encompassed that portion of the Information Technology (IT) infrastructure we defined as the FCC's web presence. The web presence is the architecture that includes all hardware, software, and network infrastructure that comprises the Commission's Internet entry and egress points.

The hardware that we reviewed all contributed in providing security to the FCC's web presence. Appendix A, FCC Web Presence Architecture, High Level Overview, provides a high level illustration of the FCC's web presence infrastructure. Our review included those network devices illustrated in Appendix A, such as firewalls, routers, hosts, and switches. Finally, our review encompassed both the Auctions and ITC infrastructure.

The hosts we reviewed were primarily located in the Demilitarized Zones (DMZ) of the ITC and Auctions systems. The DMZ refers to a complex multiple machine firewall setup, where a computer is placed outside the firewall, but is still available for use by the internal (protected) network. The advantage of a DMZ computer is it can use and receive information from the entire Internet. The disadvantage is that the DMZ may be vulnerable to attack from parties unknown.[1] As Appendix A illustrates, the ITC modified their DMZ by placing the DMZ hosts between an outer and an inner firewall.

Our audit of the web presence infrastructure also included a review of operating system controls of the DMZ hosts. This review was performed to determine if any vulnerabilities existed that could allow intruders unauthorized access through the web presence architecture and included penetration testing. We also reviewed selected application program controls in FCC electronic filing (e-filing) systems that allow users electronic access to Commission data and information. The controls we reviewed included password standards and the use of encryption in e-filing systems. These e-filing systems include applications for license or tariff filing or renewal, fee payment and Auctions bidding procedures.

The scope of our audit was limited to the FCC's web presence. No database systems or servers were reviewed. No controls over Intranet sites were reviewed.

We performed a limited review of application controls on e-filing systems. This encompassed a review of userIDs and passwords and the use of encryption to transmit data over the Internet. We reviewed backup and contingency planning procedures of e-filing applications. We did not review enterprise backup and contingency planning procedures.

The audit was conducted at the Commission headquarters facility located at 445 12$^{th}$ Street, Southwest, Washington, DC. Fieldwork on this audit was conducted from February 25, 2000 through January 30, 2001.

## AUDIT APPROACH

The Technical approach was based on the audit methodology found in the General Accounting Office (GAO) Federal Information Systems Control and Audit Manual (FISCAM), dated, January, 1999. This manual covers the essential requirements for evaluating the Commission's information systems general controls procedures. We also used contractor proprietary procedures to augment the FISCAM.

[1] DSL Reports, Knowledge Base, URL:http://www.dslreports.com/information/kb/DMZ. (March 6, 2001).

Our evaluation focused on two (2) of the six (6) FISCAM general controls categories as they applied to web presence activities:

- Access controls limit or detect access to computer resources (data, equipment, and facilities), thereby protecting these resources against unauthorized modification, loss, and disclosure[2].

- System software controls limit and monitor access to the powerful programs and sensitive files that control the computer hardware and secure applications supported by the system[3].

We also incorporated selected portions of the FISCAM sections addressing service continuity and application software development. Service continuity controls ensure that, when unexpected events occur, critical operations continue without interruption, or are promptly resumed and critical and sensitive data are protected. We performed a limited review of service continuity controls as the related to selected e-filing applications.

Application software development and change controls prevent unauthorized programming or program modifications. An assessment of the coding of Application Controls was beyond the scope of this review. The extent of the application controls review was limited to information obtained by interview and by assessing common techniques used to protect data during transmission and while obtaining access.

Under our approval and supervision, TWM used proprietary tools and audit procedures to perform complex technical analyses. This combined approach also addressed many of the general controls contained in OMB Circular No. A-130, Appendix III.

The audit team consisted of the following members:

| | |
|---|---|
| Thomas Bennett | FCC, Office of Inspector General |
| Walter Opaska | FCC, Office of Inspector General |
| Ian M.Harper | TWM Associates, Inc. |
| Dave Elliott | TWM Associates Inc. |
| Jeff Sullivan | TWM Associates, Inc. |

The audit included the following three phases:

> *Internal Controls Phase*--to develop an understanding of the organizations, operations, and activities related to the program and system, and identify the potential risks to determine the extent of detailed analyses and testing necessary;

[2] United States General Accounting Office, Federal Information Systems Control and Audit Manual, Volume 1, January, 1999, p.3-1.
[3] Ibid., p.3-2.

*Testing Phase*--to accomplish the detailed analyses and testing steps necessary to complete the audit; and

*Reporting Phase*--to formally report the results of the audit, including conditions, causes, effects, criteria, conclusions (when warranted) and recommendations.

**Step One: Internal Controls Phase**

*Objective: The objective of this step was to identify previous audits, existing design, implementation, and operational documents that describe the business processes, organizations, and security policies associated with the FCC Web Presence.*

During this phase, the audit team focused on gathering information on FCC policies, previous OIG or other regulatory audit reports and reviews, and design, implementation and operational audit documents for the FCC Web Presence. As part of this effort the Web Presence OIG Audit team requested information on various aspects of the function and composition of systems providing Web-based resources.

**Step Two: Testing Phase**

*Objective: The objective of this step was to verify the security posture of the FCC systems providing information via the World Wide Web and to identify security weaknesses in the general controls and application development techniques in the areas of access controls, network security, and system software.*

In Phase 2, Testing, The audit team: (1) assessed the current security posture of the Commission-wide systems providing information via the Web; (2) identified vulnerabilities in the General Controls; and (3) reviewed application development techniques to ensure that the FCC is not vulnerable to known Web-based attacks.

**Step Three: Reporting Phase**

*Objective: The objectives of this step were to report observations in control weaknesses associated with the FCC Web Presence within the context of periodic status reports and final audit test report. This report is the manifestation of this step.*

In Phase 3, Reporting, the audit team prepared status reports, presentations, and meeting notes. These documents reflected the current state of the FCC Web Presence audit effort. This step included the production of the draft reports and final Audit Report. The final report contains all observations, recommendations, and findings.

BACKGROUND

Federal agencies are required by law to protect information resources and assets under their control. Public laws, Office of Management and Budget (OMB) circulars and memorandums, Presidential Decision Directives (PDDs), and National Institute of

Standards and Technology (NIST) publications, enumerate the federal information security framework for agencies, such as the FCC. Also, the Commission has its own guidelines that are incorporated into an FCC directive on information security.

A number of public laws deal with information security. For example, the Computer Fraud and Abuse Act of 1986 (PL 99-474) prohibits unauthorized or fraudulent access to government computers and establishes penalties for such access. Other laws of general application that apply to the protection of information resources include the Computer Security Act of 1987, the Paperwork Reduction Act of 1995, the Clinger-Cohen Act of 1996, and the Government Information Security Reform Act.

OMB circulars and memorandums provide direction as to how federal agencies are to implement these privacy laws. Appendix III of OMB Circular A-130 discusses the security of Federal Automated Information Resources. Appendix III "establishes a minimum set of controls to be included in Federal automated information security programs; assigns Federal agency responsibilities for the security of automated information; and links agency automated information security programs and agency management control systems[4]." Other OMB circulars and memorandums that apply to information security include Circular A-123, Management Accountability and Control, Memorandum M-99-18, Privacy Policies on Federal Web Sites, and Memorandum M-00-13, Privacy Policies and Data Collection on Federal Web Sites. These OMB documents add details that assist departments and agencies in implementing the laws related to privacy in the Internet environment.

Presidential Decision Directives specify agency responsibilities in specific areas. PDD 63, Protecting America's Critical Infrastructures, specifies agency responsibilities for protecting the nation's infrastructure[5]. Another, PDD 67 Enduring Constitutional Government and Continuity of Government, has sections that relate to continuity of operations planning[6].

NIST publications provide clarification of federal security principles. NIST Special Publication 800-12, Computer Security, provides assistance in securing computer-based resources by explaining important concepts, cost considerations, and the interrelationships of security controls[7]. Other relevant NIST publications include NIST Special Publications 800-4, Computer Security Considerations in Federal Procurements, 800-14, Security Considerations in Computer Support and Operations Standardized Log-on Banner, and 800-18, Guide for Developing Security Plans for Information Processing Systems. Many of the Federal Information Publishing Standards (FIPS) series published by NIST are also useful. For example, FIPS Publication 112, Password Usage, defines

---

[4] Office of Management and Budget Circular No. A-130, Management of Federal Information Resources, February 8, 1996. URL: http://www.whitehouse.gov/omb/circulars/a130/a130.html. (March 13, 2001)

[5] CIO Council, Federal Information Security Assessment Network, November 28, 2000. http://cio.gov/docs/federal_it_security_assessment_framework.htm. (February 2, 2001).

[6] Ibid.

[7] Introduction to Computer Security: The NIST Handbook, URL: http://www.claitors.com/prf/catelog/003-003-03374-0.html. (March 13, 2001).

the security metrics for passwords and specifies minimum security criteria for access control systems based on passwords[8].

We relied on the FCC Security Directives as a primary security authority. FCC Directive 1479.1, Computer Security Program Directive, establishes policy and assigns responsibilities for assuring that there are adequate levels of protection for all FCC computer systems and information created, stored, or processed, therein[9]. This comprehensive computer security document was used as one of our key criteria when performing this review.

## OBSERVATIONS

Our review found that the FCC had an active and generally effective program for managing the security of the Commission's Web Presence. During our audit, we found that the Commission has implemented numerous computer security controls designed to protect and preserve its web-based assets.

Although the Commission has implemented numerous controls, we identified thirty-eight (38) findings that impact the effectiveness of the Commission's program. These findings occurred in the areas of host and network access, system software, service continuity, and application software development controls. We recommend that the problems we identified be corrected to strengthen the security of the Commission's web presence. Our recommendations will correct present problems and minimize the risk that future security problems will occur in the FCC's Internet web presence.

Appendix B, Detailed Finding and Observations, lists the observations and recommendations from the review of the FCC Web Presence. Because of the sensitivity of the observations, we classified have Appendix B as privileged and confidential, for internal FCC use only and will release that appendix only to those FCC personnel with a need for the information.

## RESPONSE

The two entities primarily responsible for the security of the FCC's Web Presence, the Wireless Telecommunications Bureau (WTB) and the Information Technology Center (ITC), prepared separate responses to the draft report and its thirty-eight (38) findings. In the WTB response, the Chief, WTB, concurred with the with the recommendations for the twenty (20) findings that applied to the bureau. Of these twenty (20) findings, WTB reported that fifteen (15) were closed as of May 7, 2001. We have included a copy of the response from WTB in its entirety as Appendix C to this report.

---

[8] FIPS Listed by Number, August 11, 2000. URL: http://www.itl.nist.gov/fipspubs/by-num.htm. (March 14, 2001).

[9] FCC Instruction 1479.1, Computer Security Program Directive, November 30, 1995, URL: http://intranet.fcc.gov/omd2/docs/directives/fccinst1479_1.html. (March 14, 2001).

In the ITC response to the draft report, the Chief Information Officer (CIO) concurred or concurred with comments to twenty-eight (28) of the thirty-one (31) findings that applied to ITC. The ITC disagreed with the recommendations of three (3) findings. Also, ITC requested that we reclassify the severity of a third finding, while concurring with its recommendation. In response, we have added our comments to the end of these four (4) findings. We have included a copy of the response from ITC in its entirety as Appendix D to this report. Where ITC disagreed with our conclusions, we have added a section titled "OIG Comments," where we explain our position.

ITC also stated that the concurrence and completion dates associated with each of the respective IG recommendations is conditional prior to the completion of a cost, staffing and impact analysis for each of the action items provided in your report. The cost analysis is being formulated and will be shared with the IG office once approved by the CIO. As of the date of the issuance of this report, the OIG has not received this cost, staffing, and impact analysis.