REPORT ON THE AUDIT OF NETWORK REMOTE DIAL-IN SECURITY

TABLE OF CONTENTS

Page

EXECUTIVE DIGEST 1

AUDIT OBJECTIVE 4

AUDIT SCOPE 4

BACKGROUND 4

FINDING - The Commission Has Not Adequately Secured The Network Remote Dial-In Capability

- o Details of Finding 7
- o Recommendations 11

APPENDIX 1 - Audit Team and Acknowledgements

APPENDIX 2 - Audit Methodology

APPENDIX 3 - October 18, 1996 report entitled "Flash Report on Vulnerabilities Identified during our Review of Remote Dial-In Security"

APPENDIX 4 - January 10, 1997 report entitled "Audit Of The Federal Communications Commission (FCC) Remote Dial-In Capability" prepared by TWM Associates, Inc. reporting the detailed results of Remote Dial-In Testing

APPENDIX 5 - Managing Director's Response to the Draft Audit Report

EXECUTIVE DIGEST

In 1992, the Commission engaged in an agency-wide effort to modernize its automated information systems. The goal of the program, entitled "Information Systems Modernization (ISM)", was to "replace the Commission's obsolete IRM [Information Resource Management] equipment and systems with an entirely new information systems architecture to meet our mission needs." Many objectives were envisioned including "easier access to all databases and greatly enhanced ability to retrieve and to manipulate data to support regulatory and administrative decisions" and "widespread use of electronic mail and bulletin boards for dissemination of information, exchange of documents, and communications within the Commission and with the public." To accomplish these objectives, the Commission moved from a centralized mainframe processing environment to a distributed network-based processing environment.

Since 1992, the Commission has made tremendous strides in implementing the distributed networked environment which existed only on paper at that time. In fact, the rapidity of changes in computers have resulted in accomplishments beyond those originally anticipated. For example, the introduction and encouraged use of the Internet as a means of distributing information has greatly reduced the need for bulletin boards as originally envisioned. However, along with the benefits that have clearly been derived from the Commission's conversion to a distributed environment, have come increased risks. The major risk to networked environments such as the Commission's is an unauthorized user gaining access to the network or an authorized user accessing inappropriate network resources.

As part of our ongoing efforts to ensure the security of the Commission's network, the Office of Inspector General (OIG), working closely with the office of the Associate Managing Director - Information Management (AMD-IM), has conducted an audit of network remote dial-in security. To conduct this review, the OIG contracted with the computer security firm of TWM Associates, Inc. (hereafter referred to as "TWM") to provide technical support.

The FCC Wide Area Network (WAN) supports remote access using a centralized modem pool, Novell's GroupWise Remote and Symantec's PcAnywhere for Window's communication software, and standard phone service. Depending on the type of communication software installed, modem pool users can do everything from checking e-mail to accessing databases. In addition, access to the network can be gained using stand-alone modems and analog phone service. This method of access includes both known entry points (modems purchased and distributed by AMD-IM) and unknown entry points (modems purchased and installed without AMD-IM's knowledge). The

objective of this task was to evaluate the current security configuration of modem pool dial-in security and, as needed, define an enhanced security posture. An additional objective was the identification of unknown dial-up entry ports supporting stand-alone modem access (i.e.,"rogue" modems), an assessment of the security of those ports, and the identification of alternatives for securing those ports (please refer to figure 1 below).

figure 1 - Series of stand-alone modems collected from network hub rooms

During our review, we determined that the Commission's network is vulnerable to compromise via remote dial-in. In fact, during testing the audit team was able to gain access to the network and compromise a limited number of components. In our opinion, given time and using readily available automated tools[1], the audit team could have compromised additional components of the network and

[1]The audit team chose not to use these tools because of concerns about compromising network integrity. In addition, testing the logical security of internal network components was not an objective of this review.

affected its overall integrity, confidentiality, and availability. Due to the severity of the specific condition identified during testing, the OIG issued a report entitled "Flash Report on Vulnerabilities Identified during our Review of Remote Dial-In Security" during the audit. A copy of the flash report is included as Appendix 3 to this report.

In addition to the specific vulnerabilities identified in our flash report, we determined that Commission equipment and telecommunication inventory records do not accurately reflect distributed modems; telecommunications resources are not physically secured; selected network components are not properly configured and administered to ensure secure use; and security violation logs are not adequately monitored.

As we have stated, the Commission has become increasingly dependent upon its automated systems. Interruption to services provided by the network, which include access to databases, e-mail, and the Internet, would be extremely disruptive to the Commission. Loss of the network would have an immediate and profound effect on employee productivity and would impact the Commission's ability to service its customers. For example, the e-mail system could be disabled, information available on Commission databases could not be retrieved, or distribution of public information could be hampered. Strong controls over the network remote dial-in capability, particularly over "rogue" modems, help create a secure environment and reduce the risk of these scenarios.

Detailed information about the methodology used, specific conditions identified, and other sensitive material collected in this review is included in a series of appendices attached to this report. Those appendices containing sensitive information are hand stamped "SENSITIVE" and will be distributed only to those personnel with a need for the information. Those personnel receiving these appendices are requested not to photocopy or otherwise distribute this material.

AUDIT OBJECTIVE

The Federal Communications Commission (FCC) has established access to the internal Wide Area Network (WAN) through remote dial-up connectivity allowing FCC users to access the network from remote locations using laptop or stand-alone personal computers via a centralized modem pool. The objective of this audit was to evaluate the current security configuration of this dial-in capability and, as needed, define an enhanced security posture for the existing configuration. An additional objective was the identification of unknown dial-up entry ports (supporting stand-alone "rogue" modems), an assessment of the security of those ports, and the identification of alternatives for securing those ports.

AUDIT SCOPE

The audit was conducted in accordance with Generally Accepted Government Auditing Standards and included such analysis, interviews and testing as required to support the audit findings.

The scope of this review included all components of the Commission's WAN, however, our review of field office components was limited to telephone interviews and did not include a physical observation of the automated environment. In addition, our review did not include an assessment of Integrated Services Digital Network (ISDN) modems. At the time of our review, the Commission was testing a limited number of these modems.

Audit fieldwork included interaction with most Commission Bureaus and Offices and was performed from September through November 1996.

BACKGROUND

On December 24, 1985, the Office of Management and Budget (OMB) issued Circular No. A-130. This Circular provides a general policy framework for management of Federal information resources. The Circular implements provisions of the Paperwork Reduction Act of 1980 as well as other statutes, Executive Orders, and policies concerning general information policy, information technology, privacy, and maintenance of Federal records. In addition, the Circular places specific responsibility on the head of each agency to "(e)nsure that the information policies, principles, standards, guidelines, rules and regulations prescribed by OMB are implemented appropriately within the agency."

Appendix III to OMB Circular No. A-130, entitled "Security of Federal Automated Information Systems", establishes a minimum set of controls to be included in Federal automated information

systems security programs. The appendix specifically requires that agencies shall:

a. Assure that there are appropriate technical, personnel, administrative, environmental, and telecommunications safeguards in automated information systems;

b. Assure the continuity of operations of automated information systems that support critical agency functions;

c. Implement and maintain an automated information systems security program, including the preparation of policies, standards, and procedures;

d. Assure that an appropriate level of security is maintained at all information technology installations operated by or on behalf of the Federal Government.

On January 8, 1988, the President signed the Computer Security Act of 1987 into law. The purpose of the law was to recognize that "improving the security and privacy of sensitive information in Federal computer systems is in the public interest." The law "creates a means for establishing minimum acceptable security practices for such systems, without limiting the scope of security measures already planned or in use."

The Commission's network remote dial-in capability is currently provided via a centralized modem pool and a special FCC-modified version of Symantec's Norton PcAnywhere for Windows and Novell's GroupWise Remote product (please refer to figure 2 on page 6). Based upon a July 1996 survey conducted by the Office of the Associate Managing Director - Information Management (AMD-IM), there are three-hundred fifty-one (351) potential Groupwise Remote users (i.e., users who have requested Groupwise Remote for their home personal computers). In addition to the AMD-IM controlled modem pool, there are an unknown number of additional analog and Integrated Services Digital Network (ISDN) modems installed by end-users (please refer to figure 1 on page 2).

figure 2 -Close-up of the centralized modem pool maintained in the Commission computer room in the 1919 M Street facility

Finding - The Commission Has Not Adequately Secured The Network Remote Dial-In Capability

During our review, we determined that the Commission has not established effective controls to ensure the security of the network remote dial-in capability. For example, we determined that Commission equipment and telecommunication inventory records do not accurately reflect distributed modems; telecommunications resources are not physically secured; selected network components are not properly configured and administered; and security violation logs are not adequately monitored.

Inadequate controls over the network remote dial-in capability threaten the viability of the network by increasing the risk of inappropriate access. During our review, we determined that the Commission's network is vulnerable to compromise via remote dial-in. In fact, during testing the audit team was able to gain access to the network and compromise a limited number of components. In our opinion, given time and using readily available automated tools, the audit team could have compromised additional components of the network and affected its overall integrity, confidentiality, and availability. Due to the severity of the condition and to ensure a timely response, the OIG issued a "Flash Report." A copy of the flash report, entitled "Flash Report on Vulnerabilities Identified during our Review of Remote Dial-In Security" and dated October 18, 1996, is included as Appendix 3 to this report.

Requirements For Securing The Remote Dial-In Capability Are Well Established In Government, Industry And Commission Standards

The requirements for securing network connectivity are well established in Government and industry standards. Office of Management and Budget (OMB) Circular No. A-130, entitled "Management of Federal Information Resources", establishes a minimum set of controls to be included in Federal automated information systems security programs. The Circular states that agencies shall "assure that there are appropriate technical, personnel, administrative, environmental, and telecommunications safeguards in automated information systems" and that agencies "assure the continuity of operation of automated information systems that support critical agency functions."

In December 1990, the Institute for Internal Auditors published the *Systems Auditability and Control Report*, hereafter referred to as the "SAC Report." The SAC Report is the result of a major research project conducted by top professionals in the information systems audit profession and provides comprehensive guidance on information technology and information systems auditing. Requirements for network remote access controls are recognized in several modules of the SAC Report. In module

eight, entitled "Telecommunications", the SAC Report recognizes dial-in security as a "major means of network control" to "prevent an unauthorized user from gaining access to the network through a combination of hardware, software, and physical security." The module goes on to state that "(t)he likelihood of an unauthorized user accessing the network through the telephone line is directly related to the ease of determining the network port's telephone number, the costs incurred while attempting this action, and the effectiveness of logical security barriers. When the network access number is easy and inexpensive to obtain and logical security controls are inadequate, the possibility that an unauthorized user will attempt to breach network security is relatively high" (emphasis added). In fact, these conditions were identified during our testing of remote dial-in security.

FCC Directive 1479.1, entitled "FCC Computer Security Program" and dated November 30, 1995, establishes a framework of guidelines for remote dial-in at the Commission. The directive states that the "guidelines should be considered by FCC users and AMD-IM Network Administrators to facilitate secure dial-in/out communication with FCC computer systems." The following guidelines are provided:

- Dial-in ports should be protected from unauthorized access;
- Dial-in to FCC computer systems must only occur through entry points approved by AMD-IM;
- Updates and changes in system communication hardware and software should be tested thoroughly to prevent unintentional access exposures;
- Controls should be established to ensure remote users are positively identified and authenticated before connection to the network is authorized. Further, remote system(s) access using Guest accounts must be prohibited; and
- Reasonable care should be taken to protect communication equipment and telecommunications cables from unauthorized access. Any installation or adjustment of communication equipment must be coordinated through AMD-IM, NMD [Network Management Division] in advance.

In our opinion, these guidelines present a solid framework for managing network remote dial-in security. The audit team found little evidence of the implementation of these controls during our review.

Commission computer equipment and telecommunications inventory records do not accurately reflect distributed modems

As part of our review of remote dial-in security, we obtained and reviewed copies of computer equipment and telecommunication inventory records. Using these records, the audit team conducted a physical survey of Commission work space. The objective of the survey was two-fold. The first objective was to locate modems and the second objective was to assess the accuracy of inventory records. During the review, we located numerous modems which did not have FCC inventory tags and which were not reflected in the equipment inventory.

Telecommunication inventory records identify both ISDN and analog phone lines. In general, ISDN lines support Commission voice service and analog lines support fax machines, secure phones, and modem resources. The audit team obtained an automated copy of the telecommunication inventory records and developed a report, sorted by physical location, of analog lines. In addition to physically tracing analog phone lines to test accuracy, the audit team used "war dialer" software to call several thousand Commission extensions. As a result of this testing, the team identified numerous modems which were not accurately recorded in telecommunications inventory records. Detailed results of our testing is provided in Appendix 4 of this report.

Telecommunications resources are not physically secured

In March 1994, the OIG issued an audit report entitled "Report on the Audit of Physical Security of the Local Area Network." In that report, the OIG reported weaknesses in the physical security of areas, including telephone closets used for vertical cabling, where critical network components are stored. In that report, we recommended that steps be taken to ensure that these areas are secured. In March 1996, the OIG issued an audit report entitled "Report on the Follow-Up Audit of Physical Security of the Local Area Network." In that report, the OIG reported that weaknesses in physical security in areas where critical network components are stored continue to exist and recommended that steps be taken to ensure that these areas are secured.

As part of our review of remote dial-in security, we conducted a physical survey of Commission work space in the Washington, DC area and at the Gettysburg, PA. facility. The Washington D.C. locations included:

- 2000 L Street
- 1919 M Street
- 2000 M Street
- 2025 M Street
- 2033 M Street
- 2100 M Street
- 1250 23rd Street

During our review of work space in the Washington, DC. area we identified several phone closets containing both telecommunications wiring and network cabling which were not physically secured. In addition, we identified numerous ISDN handsets (telephones) stored in these unsecured areas. These ISDN handsets are valued from $500 to $800 per unit.

Selected Network Components Are Not Properly Configured

As part of our assessment of remote dial-in security, we used "war dialer" software, as well as computer equipment and telecommunication inventory records, to identify network ports supporting remote communication. Following identification, we conducted off-site tests to assess the security of those ports. Standard login procedures were used in an attempt to "break into" the system. In addition to assessing these ports, we evaluated security of the modem pool supported by AMD-IM.

During testing, we identified several weaknesses in the configuration of network components. For example, we were able to compromise a network component that was configured to allow GUEST logins. Using this component as an attack platform, we were able to compromise additional network equipment which allowed GUEST login. In addition, we identified network components which were not configured to require userids and passwords. In our opinion, this equipment could have been "captured" by the audit team by simply establishing a User ID and password. The result would have been the inability of network management personnel to gain access to this equipment. Detailed results of our testing is provided in Appendix 4 of this report.

Security Violation Logs Are Not Adequately Monitored

As reported in the previous finding, we conducted off-site testing of identified network ports supporting remote dial-in. Initially, the testing was conducted after Commission business hours to reduce the likelihood of identification by network management personnel. However, after several successful attacks against the network, the team decided to conduct testing openly during business hours. Our intent in conducting tests during business hours was to assess the degree to which network management personnel were able to review security logs and report security incidents in a real time manner. Our testing indicated that security violation logs were not being adequately monitored.

Remote Dial-In Security Weaknesses Threaten Network Viability

Inadequate remote dial-in security increases the risk of inappropriate access and threatens the availability, integrity, and confidentiality of information on the network. During our

testing, we demonstrated the vulnerability of the network to inappropriate access by remote dial-in. After successfully compromising one inappropriately configured computer, the audit team was able to attack and compromise several additional network components. In our opinion, the audit team gained enough privilege to compromise components of the network and affect its overall integrity, confidentiality, and availability.

Recommendation for Corrective Action 1 of 3

The Managing Director implement and *enforce* the remote dial-in guidelines established in FCC Directive 1479.1, entitled "FCC Computer Security Program." In addition, the Managing Director: (1) conduct a complete inventory of Commission modems and adjust inventory records to reflect this action; (2) require justification for the use of each modem identified; (3) assess the security and operational requirements of each modem for which a valid requirement exists; (4) remove modems for which no valid requirement exists; and (5) establish a program for periodically testing modems to ensure that an acceptable level of network security is maintained.

Recommendation for Corrective Action 2 of 3

The Managing Director take steps to physically secure areas where critical telecommunications resources are stored.

Recommendation for Corrective Action 3 of 3

The Managing Director address the specific conditions reported in Appendix 4[2]. In addition, the Managing Director examine all network components to ensure that: (1) all components employ unique individually assigned userids and passwords; (2) adequate security features including password files and audit files are implemented and protected; and (3) access to sensitive communication applications be limited. Furthermore, the Managing Director direct network management personnel to establish a program for daily review of security incident logs.

Management Response

The Managing Director concurred with the report results and provided specific comments about selected conditions identified during the review. With respect to our finding of Guest account login with no password, the Managing Director reports that this capability has been disabled. In addition, the Managing Director

[2]Because of the sensitive nature of the material contained in this document, copies will only be distributed to those personnel with a need for the information.

reports that two components accessed during the review, "Maglink1" and "Maglink2", are "bridges which were previously used to support network connectivity" and that "these devices are not physically connected to the network." The Managing Director goes on to state that "since the devices are kept in inventory for contingency use, AMD-IM has coordinated an effort to take precautionary measures and now require a password for future use of the devices."

With respect to our finding that dynamic userid/password files created by GroupWise can be recovered using Norton Utilities, the Managing Director explains that "the threat is minimized by the fact that successfully hacking one computer will only allow access to the last GroupWise e-mail account accessed from that computer." Furthermore, the Managing Director points out that "to accomplish such a break-in, a person would require physical access to the space where a computer is located."