

REPORT ON THE FOLLOW-UP AUDIT OF PHYSICAL
SECURITY OF THE LOCAL AREA NETWORK

Table of Contents

	<u>Page</u>
EXECUTIVE DIGEST	1
AUDIT OBJECTIVE	3
AUDIT SCOPE	3
BACKGROUND	3
FINDING No. 1 - Weaknesses Continue To Exist In The Physical And Environmental Security of Critical Network Hardware	
o Details of Finding	5
o Recommendations/Management Response	13
FINDING No. 2 - Inadequate Management of Laptop Computer Resources	
o Details of Finding	15
o Recommendations/Management Response	20
APPENDIX - Managing Director's Response to the Draft Audit Report	

EXECUTIVE DIGEST

In March 1994, the Office of Inspector General (OIG) issued an audit report entitled "Report on the Audit of Physical Security of the Local Area Network." In that report, the OIG concluded that the Federal Communications Commission (FCC) had not established internal controls which adequately protect components of the FCC network from physical and environmental threats. Such physical and environmental threats to the network include deliberate intrusion, natural and/or man-made hazards, damage or theft of equipment, and unauthorized access to data.

The objective of this audit was to determine whether the Commission had implemented a corrective action program in response to our March 1994 audit report. An additional objective was to evaluate the controls in place to ensure the protection of network microcomputer workstations and laptops from physical and environmental threats.

During the review we found significant improvements in the Commission's computer security program. For example, in our March 1994 report we reported that the Commission had not conducted a risk analysis or prepared a computer security plan for the network as required by the Computer Security Act of 1987.

During this review we examined the Commission's risk assessment and security planning activities and determined that a network risk assessment was completed and a comprehensive security 2-year plan has been developed based, in part, on that assessment. In addition, the Commission issued a final version of Directive FCCINST 1479.1 entitled "FCC Computer Security Directive." This Directive provides a comprehensive framework for managing computer security on the variety of hardware and software platforms used by the Commission.

Although we recognize significant progress in the Commission's computer security program, we found that further improvements in physical and environmental security controls are necessary to adequately protect the network from physical and environmental threats. In addition, our review identified weaknesses in the management of laptop computers.

The FCC has become increasingly dependent upon its automated systems. Interruption to services provided by the Local Area Network (LAN), which include access to databases, E-mail, and the Internet, would be extremely disruptive to the Commission. Loss of network and portable computing resources would have an immediate and profound effect on employee productivity and would impact the Commission's ability to conduct business. This would include the Chairman, Commissioners, and their respective staffs.

For example, the E-mail system would be disabled and information on Commission databases could not be retrieved. Physical and environmental controls, i.e., locks, fire extinguishers, uninterruptable power supplies (UPS), etc., help ensure that these scenarios do not occur. These measures can be readily

adopted at a reasonable cost and, in the case of fire extinguishers and UPS, are transportable within the current FCC space or to the Portals as is projected for mid-1997.

The Managing Director has concurred with each of our recommendations and has provided a timetable for implementing corrective action. Excerpts from the Managing Director's response to our draft report are incorporated under the appropriate audit recommendation. The entire response is contained in the Appendix to this report.

AUDIT OBJECTIVE

The first objective of this audit was to determine the status and effectiveness of corrective actions which were instituted as a result of recommendations contained in a March 1994 OIG audit report entitled "Report on the Audit of Physical Security of the Local Area Network." An additional objective was to examine the physical and environmental security of network microcomputer workstations and laptop computers.

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 was limited to the network and microcomputer workstations operating in FCC Headquarters office space. The scope of our assessment of physical and environmental security of laptop computers was not geographically limited (i.e., laptop computers assigned to field components were included in the review).

Audit fieldwork was primarily performed within the Office of the Managing Director (OMD) from October 1995 through February 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."

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 concluded that the Commission had not established internal controls which adequately protect components of the FCC network from physical and environmental threats. In addition, the OIG concluded that this condition resulted in an increased risk and magnitude of harm that could result from a wide variety of physical threats and environmental hazards to the network including deliberate intrusion, natural and/or man-made hazards, damaged or stolen equipment, and unauthorized access to data.

Finding No. 1 - Weaknesses Continue To Exist In The Physical
And Environmental Security of Critical Network
Hardware

In the "Report On The Audit Of Physical Security Of The Local Area Network," dated March 30, 1994, the OIG reported the results of our tests of physical and environmental security in computer hub rooms in the 1919 M Street headquarters facility. For purposes of this review, we have defined a computer hub room as an area containing core network hardware (e.g., file servers, routers, patch panels, etc.). The report concluded that the Commission had "not established adequate physical security controls to protect critical LAN hardware from physical threats."

In addition, we concluded that "(t)he FCC has not protected some critical LAN components from environmental hazards." We recommended implementation of a series of controls to improve the physical and environmental security of network hardware. Management concurred with our recommendations and established a time table to effect the action required to correct the identified deficiencies.

As part of this review, we examined the corrective action taken by the Commission to improve physical and environmental security in computer hub rooms containing network equipment. In addition to assessing managements activity resulting from our March 30, 1994, audit report, the scope of this follow-up review was expanded to include hub rooms in the following FCC headquarters office space:

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

During the review, we identified physical and environmental security weaknesses which had been identified and reported in our previous audit. During audit testing, we identified the following conditions: (1) computer hub rooms, including the FCC data center, which were not physically secured during and after business hours; (2) hub rooms which did not employ cypher locks on all points of entry nor deploy additional security devices (e.g., door locks) when those devices were available; (3) hub rooms in which equipment was not properly protected from accidental disconnection; (4) lack of smoke detection and fire suppression in computer hub rooms; (5) hub rooms which showed signs of water damage; and (6) hub rooms which were excessively dirty.

Inadequate physical and environmental security controls threaten the viability of the network by increasing the risk of damage to

equipment (whether willful or inadvertent), theft of equipment, and unauthorized access to data.

These conditions resulted from: (1) physical space restrictions during network installation requiring commingling of network equipment with common work areas and items; (2) lack of employee awareness of security requirements; (3) budget restrictions; and (4) inadequate planning for physical and environmental security during expansion.

Requirements For The Physical And Environmental Security Of Critical Network Resources Are Well Established By Government Regulation And Industry Standards

The requirement for physical and environmental security of computer equipment is addressed in Federal and Agency regulation.

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." Furthermore, FCC Directive 1479.1, entitled "FCC Computer Security Program", addresses guidelines for the protection of FCC computer systems. The Directive establishes that "offices and work areas where FCC computer systems are located must be physically secured when unattended." The Directive recognizes that "(a)dequate controls should be employed consistent with the value, exposure and sensitivity of the information and equipment that is to be protected."

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 strong physical and environmental security are recognized in several modules of the SAC Report. In module four, entitled "Managing Computer Resources", the SAC Report recognizes that "(a) well-designed security program addresses physical security" and that physical security "should be designed to: Prevent unnecessary and unauthorized access to the computer room and equipment; and prevent unauthorized access to computer operations areas." Module nine of the SAC Report, entitled "Security", states that "(w)ith the expanded reliance on Information System (IS) data and resources, security has become fundamental to the ongoing viability of most organizations" and

that physical security "is the most basic and commonly addressed form of IS control."

With respect to environmental security, module nine of the report discusses the risks presented by environmental hazards including fire and water damage, as well as damage from "pollutants in the air or from chemicals used in or near the environment where the information systems are located." Chapter three of this module directly addresses the need for smoke detection and fire extinguishing equipment reporting that "(f)ire and flood, along with the resultant damage caused by fire extinguishing procedures (smoke and water damage), are two of the most common causes of damage to IS equipment and records.

The Commission Has Not Provided Adequate Physical And Environmental Security For Computer Hub Rooms Containing Critical Network Components

The Commission has distributed critical network hardware to a series of rooms (hereafter referred to as "hub rooms") throughout the buildings being used by headquarters personnel. Hub rooms vary in complexity from those which contain only "patch panels" (connecting vertical and horizontal cabling) to those containing network file servers and database servers. The core components of the FCC network are located in the FCC Data Center (Room M10 of the 1919 M Street facility). Equipment in the Data Center provides network connectivity to other headquarters buildings, field offices, the Laurel laboratory, the Gettysburg facility, and the Auction site located on Massachusetts Avenue in Washington, DC. In addition, the Commission's modem pool (providing dial-in/dial-out services) and many of the network database servers are located in the Data Center.

As part of our testing of physical and environmental security controls, we:

- reviewed policies and procedures established to control access to hub rooms;
- identified the locations of these hub rooms and conducted tests, both during and after business hours, to determine the status of physical and environmental security in these areas;
- examined the security measures (e.g., cypher locks, key locks, Uninterruptable Power Supply (UPS), fire control, etc.) taken to protect computer hub rooms;
- interviewed representatives from the Office of the Associate Managing Director - Operations to develop an understanding of controls over building access and

egress;

- surveyed personnel with hub room access to determine familiarity with security requirements; and
- examined that results of self testing conducted by the FCC Computer Security Officer.

On November 21 and 22, 1995, we conducted an inspection of computer hub rooms in six FCC headquarters buildings. The inspection was conducted during business hours. During the inspection, accompanied by the FCC Computer Security Officer, we tested the physical and environmental security controls in place in twenty-six computer hub rooms. During that testing we identified the following weaknesses:

- Eight of the hub rooms inspected were not physically secure during our testing. The severity of this finding is compounded by the fact that, during the inspection, we were challenged for identification on only one occasion by an FCC employee. In fact, in several cases we were directed to unsecured hub rooms by helpful FCC personnel. It should be noted that we did not display FCC identification nor were we familiar, as a rule, to persons in the areas we visited. In fact, on the second day of our inspection we were dressed in casual attire.

- Thirteen of the hub rooms inspected had one or more entry points that did not employ a cypher lock security. In some cases, these entry points were equipped with a key lock security feature that was being used at the time the testing was conducted. However, in other cases, these entry points were unsecured. In one hub room the cypher lock had been disabled to allow access to the room. In another case a sign on the door warns users "Do Not Lock Door."

- Seventeen of the hub rooms inspected were being utilized as "shared" space and were not dedicated to supporting the network backbone. Many of the hub rooms contained unused furniture, file cabinets, printers, fax machines, book cases, and other non-network related materials. Use of hub rooms for purposes other than support of the network significantly increases the risk of willful or inadvertent damage to equipment, theft of equipment, and unauthorized access to data.

- In three of the hub rooms inspected, we observed cabling which was not properly protected from accidental disconnection. Two of these hub rooms were being used as "shared" space.

- None of the hub rooms inspected were equipped with smoke detection equipment.

- Six of the hub rooms inspected contained evidence of water damage. In one location there was evidence of significant water damage. Some of the damage was on the ceiling above network equipment.

- Fourteen of the hub rooms did not have a fire extinguisher within fifty feet. In fact, the only hub rooms that had this equipment nearby were those located near the elevators in the 1919 M Street building.

- A file server in one of the hub rooms was not equipped with an operational Uninterruptable Power Supply (UPS). UPS equipment provides backup in the event of a power failure. In addition, we observed cleaning solvents stored in this hub room. Fumes from these solvents may cause damage to sensitive network components. In addition to solvents, we observed that many of the hub rooms inspected were not properly maintained. Many of the rooms contained old newspapers, magazines, food containers, etc.

For security reasons, we have provided the Managing Director with a comprehensive listing of hub rooms tested and weaknesses identified by location under separate cover.

The FCC Data Center Was Not Physically Secured After Business Hours

The core of the FCC's information network is located on the mezzanine level of the 1919 M Street facility. Specifically, the data center contains numerous network file servers, data base servers, telecommunications equipment, network hub equipment, and backup equipment. Traditionally, due to the sensitivity of the data maintained at such a site, high value of the equipment, and environmental sensitivity, control over access is carefully administered. In fact, access via card key, cypher locks, and use of biometric devices are routine in many data centers.

On December 12, 1995, representatives from the OIG went to the data center to evaluate the physical security of the workstations. Expecting stringent access security, the auditors were surprised to discover no hindrance to entrance. After gaining entrance, the auditors toured the data center looking for on duty personnel. No personnel were found in the area. During a second visit later that evening, auditors observed and photographed numerous network file servers (including a file server "mirroring" the auction file server), telecommunications equipment, UNIX data base servers (figure 1 on page 11), boxed UNIX equipment, numerous personal computers, and other computer equipment.

During our inspection of the data center, we noted access from the data center to the loading dock in the rear of the 1919 M Street building existed via an elevator. At the time of our visit, we observed that the elevator latch was in place and that the elevator was secure (figure 2 on page 11). However, in a previous building security tour, conducted with representatives from the AMD-O security office, AMD-IM, and the contract security force, we observed that: (1) this elevator was not secured while not in use, and (2) the rear loading dock was unsecured. We were informed by a representative from the contract security force that these conditions are occasionally observed during routine security checks. In our opinion, the severity of the data center physical security weakness we identified is compounded by this weakness in building access control.

We contacted representatives from AMD-IM to determine the reason for this condition and to determine what steps would be taken to prevent a recurrence. We were informed that "a simple oversight in checking the front door was the cause of the center being left open." The AMD-IM response went on to note that "Data Center staff have been instructed to verify that all access points are secured before closing the Data Center."

On February 21, 1995, representatives from the OIG met with the FCC Computer Security Officer and were provided with an update on security enhancements in the data center. In addition, we conducted an inspection of the data center and were briefed on planned controls.

figure 1: OIG Auditor standing in front of UNIX database servers located in the FCC Data Center

*figure 2: Elevator providing access from the FCC Data
Center to the rear loading dock*

Physical And Environmental Security Weaknesses Threaten Network Viability

Risks associated with inadequate physical and environmental security controls include: unauthorized access to computer equipment; possible willful or inadvertent loss or destruction of equipment; and theft, unauthorized copying, modification, or destruction of data. The risk is compounded by the accessibility to FCC work areas by non-FCC personnel such as contractors, messengers, and cleaning personnel. In addition, a tested Continuity of Operations Plan (COOP), normally a significant mitigating control feature, has not been developed for the FCC network. A recently published 2-year computer security plan indicates that COOP development efforts will begin in the 3rd quarter of FY96.

Several Conditions Have Prevented Implementation Of A Strong Physical And Environmental Security Control Program

The weaknesses identified have resulted from several conditions including: (1) space restrictions which have impacted unfavorably upon secure network installation; (2) lack of employee awareness of security requirements; (3) budget restrictions; and (4) inadequate planning for physical and environmental security during expansion.

In our initial review of network physical security (as reported in our audit report dated March 30, 1994), we questioned AMD-IM management about the use of "shared" space for network hub rooms.

We were informed that many of the rooms being used are "controlled by the various Bureaus" and that "(t)hese rooms were the only rooms made available by the B/O, several years ago when OMD asked for space to put in their Departmental Computers." We were further informed that "(t)here was and still is no space on these floors to make as secure an area as desired." We stated in that report that "the importance of reducing the risk ... outweighs any inconveniences that might be imposed." We continue to hold this opinion.

During our inspection of hub rooms throughout FCC headquarters work space we were repeatedly directed to hub rooms by FCC personnel without being challenged for identification. In our opinion, this indicates a lack of awareness on the part of FCC personnel of their security responsibilities. FCC Directive 1479.1, entitled "FCC Computer Security Program," establishes these responsibilities and states that "FCC users have a responsibility to create and maintain a secure work environment, and to protect the computer assets used to fulfill business activities."

Improvements Have Resulted Since OIG Report Issuance

The Commission's computer security program has seen significant improvement since our March 1994 audit. For example, the Commission has issued a network risk assessment and a comprehensive security 2-year plan. In addition, the Commission issued a final version of Directive FCCINST 1479.1 entitled "FCC Computer Security Directive." This Directive provides a comprehensive framework for managing computer security on the variety of hardware and software platforms used by the Commission. Unfortunately, several of the planned security activities that impact physical and environmental security are on hold because of funding problems. For example, Continuity of Operations Planning activities will be delayed until budget resolution. In addition, we were informed that "the need for fire extinguishers in some Hub Rooms requires funding which is currently unavailable."

The scope of our March, 1994, audit report was limited to computer hub rooms in the 1919 M Street building. In that report, we made specific recommendations for the implementation of physical and environmental security controls for those hub rooms where weaknesses were identified. During testing conducted as part of this review, we noted that the controls recommended for 1919 M Street hub rooms had been implemented. However, physical and environmental security does not appear to have been adequately addressed during the establishment of hub rooms in headquarters expansion facilities.

Planned FCC Move To Portals

The OIG recognizes that many of the concerns addressed in this report will be negated when the Commission moves to new office space in the "Portals" facility. However, in our opinion, the risks associated with the conditions we have identified in this review require that action be taken to protect network equipment prior to that move.

Recommendation for Corrective Action 1 of 4

The Managing Director take immediate steps to ensure the physical security of areas in which critical network resources are located. These steps should include (1) resolution of the shared space issue by either physical isolation of equipment within the shared space or removal of non-network materials from the area; and (2) installation of cypher locks in all hub rooms containing network hardware. In addition, we recommend that the Managing Director take steps to periodically remind FCC personnel of their security responsibilities.

Management Response

The Managing Director has concurred with the recommendation and has recognized actions taken by AMD-IM to improve physical security in computer hub rooms. In addition, the Managing Director stated that "AMD-IM and the Associate Managing Director - Operations (AMD-O) staff are installing cipher locks in key network spaces not currently equipped with such devices" and that "(b)oth groups are also working to improve existing physical security in M10, the Data Center."

Recommendation for Corrective Action 2 of 4

The Managing Director take immediate steps to ensure the environmental security of areas in which critical network resources are located. These steps should include (1) installation of smoke detection equipment in computer hub rooms; (2) installation of fire extinguishers in computer hub rooms; (3) evaluation of alternatives for periodically cleaning hub rooms; (4) evaluation of alternatives to minimize water damage exposure (including removal of equipment if necessary); (5) review of hub room cabling to minimize accidental disconnections; (6) removal of cleaning solvents from hub rooms; and (7) periodic review of the status of UPS equipment.

Management Response

The Managing Director has concurred with the recommendation and has recognized actions taken by AMD-IM to improve the environmental security of critical network components. In addition, the Managing Director has stated that "(a)ll cleaning solvents have been removed from hub rooms" and that the "periodic review of UPS equipment and its stability has been scheduled for completion by May 1996."

Finding No. 2 - Inadequate Management Of Laptop Computer Resources

Prior to 1994, a limited number of laptops had been purchased by the Commission for special purposes. In the past two years, as part of the FCC's automation initiative, the Commission has purchased over two-hundred (200) additional laptop computers. As a result, the Commission currently maintains an inventory of laptops totalling over three-hundred units. This represents approximately one laptop for every six employees. With the acquisition cost of laptops ranging from \$2,455 to \$6,149 per unit, it is clear that this equipment represents a significant capital investment. Commensurate with this investment, the Commission has not established an adequate program for managing laptop computer resources. During audit testing, we identified weaknesses which included: (1) inaccurate inventory records and (2) lack of periodic comprehensive physical inventories.

An inadequate laptop management process increases the risk of loss of scarce laptop computer resources and data. These conditions resulted from inadequate planning during program implementation.

Requirements For Managing Computing Resources Are Well Established By Industry Standards And Government Regulation

The requirement for management of portable computing resources is addressed in Federal and Agency regulation. 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 recognizes that "... the value of government information to the entire Nation, the management of Federal information resources is an issue of continuing importance to the public and to the government itself." The Circular goes on to state that agencies shall "(d) develop internal agency information policies and procedures and oversee, evaluate, and otherwise periodically review agency information management activities" and that agencies "shall assure an adequate level of security for all agency automated information systems." The circular also directs that "agency and contractor personnel involved in the management, operations, programming, maintenance, or use of information technology are aware of their security responsibilities and know how to fulfill them."

FCC Directive 1479.1, entitled "FCC Computer Security Program", addresses guidelines for the protection of portable computing resources. The Directive recognizes that "with portable computing resources there are significant inherent exposures related to theft and the safeguarding of information" and that "FCC users should be particularly security conscious when

travelling with portable computer resources." The Directive states that "offices and work areas where FCC computer systems are located must be physically secured when unattended" and that "(a)dequate controls should be employed consistent with the value, exposure and sensitivity of the information and equipment that is to be protected."

FCC Directive 1054.1, entitled "Property Management", states that it is "FCC policy to assure the proper identification, custody, use, care, maintenance and safeguarding of all Federal property."

In addition, the Directive establishes objectives which include "(t)o list and account for all inventoried Commission property at a central point within the agency" and "provide for the periodic inventory of all FCC inventoried property and reconciliation with the appropriate property records." The Directive assigns Automatic Data Processing (ADP) equipment management responsibilities to the Associate Managing Director - Information Management.

Risks associated with managing portable computing resources is addressed in several modules of the SAC Report. Module nine of the SAC Report, entitled "Security", states that "(m)icrocomputers present one of the fastest growing areas of potential data security vulnerability" and that "the most obvious form of microcomputer security is protecting the machines themselves against theft." The Report goes on to state that "(m)icrocomputers and components are now exceeding typewriters and telephones as the office equipment most often stolen. Of course, the difference is that, unlike a typewriter, microcomputers with hard disks may contain critical data that are difficult or impossible to replace."

The Commission Has Not Established An Effective Laptop Computer Management Process

In mid-1994, as part of on-going efforts to automate operations, the Commission began to procure laptop computers. Prior to that time, the Commission had purchased a small number of laptops for special purposes. Based upon our review of Commission inventory records, as of October 1995, the Commission had three-hundred seven (307) laptop computers ranging in cost from \$2,455 to \$6,149 per unit.

As part of our review of the laptop management process, we interviewed representatives from AMD-IM and Bureaus/Offices to obtain an understanding of the current laptop management process; obtained and reviewed laptop checkout documentation and associated database records; and used statistical sampling techniques to select laptop computer for detailed review.

Using a statistical model based upon a ninety-five percent (95%)

implied confidence factor and an acceptable error rate of five percent (5%), we selected a sample of fifty-four (54) laptop computers from a universe of three-hundred seven (307). For each laptop selected, we:

- used available inventory records to ascertain the organization to which the laptop was currently assigned;
- contacted the organization to determine the current location of the equipment (where available, we collected and reviewed documentation reporting equipment disposition);
- contacted the individual to which the laptop was assigned to determine if the individual had the equipment, and determine physical and environmental security controls used to protect the equipment; and
- attempted to physically verify the equipment (using recorded serial #, FCC #, and barcode information).

Our detailed review of selected laptop computers yielded the following results:

- Sixty-seven percent (67%) of the selected laptops were physically verified ($36 \div 54 = 67\%$). Verification was done through either physical examination of the equipment or, when this method was impractical, verification of Serial Number, FCC Number, and Barcode by employee. Four of the laptops in this category could not be located initially despite an extensive review of available inventory records. Information regarding these laptops was provided to AMD-IM and, through additional review, AMD-IM was able to locate the equipment.
- Eleven percent (11%) of the selected laptops could not be located ($6 \div 54 = 11\%$). Two of these laptops were reported in Help Desk inventory records as being checked out indefinitely. However, when we contacted Commission personnel reported as having checked out the equipment, we were informed that they did not have these laptops. Another laptop was reported in inventory records as having been distributed to the Compliance and Information Bureau (CIB). We contacted CIB and were informed that they were unable to locate this equipment. The FCC Computer Security Officer stated in a memorandum to the OIG that, in his opinion, "given sufficient time, the remaining laptop computers

can be located and accounted for."

- One of the selected laptops was determined to have been stolen in late November 1995. We were informed by the FCC Computer Security Officer that a copy of the Federal Protective Service report had been prepared for this equipment.
- Despite extensive efforts, we were unable to complete a physical verification of twenty percent (20%) of the laptops selected for review (11 ÷ 54 = 20%). In some cases, employees using this equipment were on travel, on leave, or out on disability during our review. However, three employees did not produce equipment for physical verification despite repeated requests to cooperate with this review effort and repeated assurances that cooperation was forthcoming.

In our opinion, the results of this detailed review of selected laptops indicate significant deficiencies in the laptop management process.

Laptop Inventory Records Are Not Accurate

The official inventory of FCC laptop computers is maintained by the Equipment Support Branch (ESB) within AMD-IM. We used their inventory report, dated October 6, 1995, as the basis for our selection of laptop computers for detailed review. Following our sample selection, we contacted Data Automation Liaison Officers (DALO) from each Bureau and Office and FCC Help Desk personnel to obtain any internal laptop inventory records that might reside in their respective Bureaus and Offices.

Starting with the official ESB inventory report we attempted to locate each individual laptop in our sample. Based upon our unsatisfactory results, we concluded that the official inventory does not accurately reflect the distribution of laptop resources to Bureaus/Offices or the Help Desk. Likewise, we determined that, certain Help Desk and Bureau/Office inventory records do not accurately reflect the physical location of the equipment.

For example, one of the laptops selected, a Toshiba 3400 CT - Serial Number 03421326, was reported in the official inventory as being assigned to the Customer Solutions Division of AMD-IM. Typically, this designation means that the equipment was assigned to the Computer Help Desk. However, in this case, no record of this equipment existed in Help Desk records. Despite extensive efforts on the part of this office and AMD-IM, we were ultimately unable to locate this equipment.

In another example, a selected laptop, Toshiba 1960 CS - Serial Number 07419506, was reported in the official inventory as being assigned to the Customer Solutions Division of AMD-IM. A review of Help Desk records indicated that the laptop had been assigned to the Help Desk and had been signed out indefinitely to an individual in the Common Carrier Bureau. We contacted the individual and were informed that he did not have this equipment. We passed this information along to the FCC Computer Security Officer who was subsequently able to locate the equipment.

It should be noted that several Bureaus and Offices did maintain accurate laptops inventory records. For example, we reviewed records maintained by the Mass Media Bureau (MMB) and found a comprehensive laptop management process.

Laptop Computer Resources Are Not Periodically Inventoried

FCC Directive 1054.1, entitled "Property Management", establishes requirements for a "periodic inventory of all FCC inventoried property and reconciliation with the appropriate property records." As part of our review, we met with a representative from the Equipment Support Branch within AMD-IM to discuss laptop inventory procedures. We were informed that the Equipment Support Branch has delegated responsibility for conducting laptop inventories to the Help Desk. We were further informed that this was the result, in part, of problems associated with conducting inventories of laptop equipment. For example, we were informed that some employees refuse to produce equipment for inventory purposes when requested. In addition, laptops are frequently moved without reporting the information to the Equipment Support Branch.

Although we were informed that periodic laptop inventory responsibilities were delegated to Computer Help Desk staff, a representative from the Computer Help Desk stated that laptops were not periodically inventoried. Instead, Help Desk inventory records are checked for accuracy when, and if, equipment is returned to the Help Desk for redistribution, repair, or enhancement. In our opinion, this process does not represent an adequate physical inventory process.

Weaknesses In Laptop Management Increase The Risk Of Asset Loss

An inadequate laptop management process increases the risk of loss of laptop computer equipment and data. As part of our review, we requested information about recent computer thefts at the Commission. We received a memorandum from the FCC Computer Security Officer documenting theft for the period from June 1995 to February 1996. During that period, seven (7) laptop

computers, valued at \$21,580¹, were reported stolen from headquarters facilities. The effect of the loss of this equipment is magnified as a result of the difficult budget conditions currently faced by the Commission. As part of this review, we have worked with the Computer Security Officer to identify potential physical control alternatives for laptops including a chip based monitoring system.

Several Conditions Have Prevented Implementation Of A Strong Laptop Management Process

In our opinion, the conditions identified in this review resulted from inadequate planning during program implementation. In mid-1994, the Commission began to purchase a large number of laptop computers. Some laptops were distributed directly to Bureaus and Offices while the remainder were assigned to the FCC Computer Help Desk. The method by which these resources were managed was left to the individual organizations. This lack of formal program establishment led to control weaknesses.

For those laptops assigned to the Computer Help Desk, management of the checkout process was originally accomplished using the Help Desk call-in log. As part of our review, we obtained and reviewed a copy of the log for 1995. The log records a variety of information about each checkout including Client Name, Organization, and Resolution. However, the log did not consistently record information about the specific laptop checked out. As part of our detailed review of selected laptops, we reviewed records from the recently developed Help Desk laptop management system. The current system is comprised of two databases, one for short term loans and one for indefinite loans.

In our opinion, this process represents an improvement over the original log process.

In addition to reviewing Help Desk records, we reviewed inventory records maintained in the Bureaus and Offices. Generally, we found that these records were well maintained. For example, we reviewed the program established by MMB and found a comprehensive program including formal policies and procedures and a database providing a detailed history of MMB's laptop inventory.

Recommendation for Corrective Action 3 of 4

The Managing Director: (1) conduct a complete inventory of Commission Laptop Computers and adjust inventory records to reflect the results of this action; and (2) decentralize the

¹ In addition, the report identifies the loss of additional automation equipment (including cellular phones, fax machines, printers, components, etc.) with a combined value of over \$57,400.

responsibility for managing laptops checked out indefinitely from the Help Desk to those Bureaus and Offices with the resources necessary to independently manage the process. The Help Desk should continue to manage laptops for those organizations who require that service.

Management Response

The Managing Director has concurred with the recommendation and stated that "(a) baseline inventory of all laptop computers has been scheduled for this fiscal year" and that "(a)s part of the corrective action, improvements for the management of laptop computers is planned."

Recommendation for Corrective Action 4 of 4

The Managing Director develop guidance for use by Bureaus and Offices managing laptop resources. This guidance should include notification to users: (1) of their responsibilities for presenting equipment for physical inspection as part of the physical inventory process; (2) of their responsibilities for ensuring the physical security of laptops that have been assigned to them and their accountability for that equipment if it is lost or damaged through their negligence; (3) that equipment is to be used only for official FCC business; and (4) that software is not to be loaded onto laptops without being scanned for viruses.

Management Response

The Managing Director has concurred with the recommendation and stated that "(g)uidance will be prepared and disseminated to Bureau and Office representatives responsible for the management of laptop computers." In referring to the guidance, the Managing Director goes on to state that "(r)esponsibilities will be outlined and users will be notified of their responsibilities when they are assigned laptop computers for official use."