FEDERAL COMMUNICATIONS COMMISSION

OFFICE OF INSPECTOR GENERAL

Report on Audit of Computer Controls
at the FCC National Call Center

Audit Report No. 00-AUD-01-12
June 21, 2000

H. Walker Feaster III
Inspector General

Thomas D. Bennett
Assistant Inspector General for Audits

Report on Audit of Computer Controls at the FCC National Call Center

Table of Contents

EXECUTIVE SUMMARY

On October 21, 1996, the Federal Communications Commission (FCC) opened the National Call Center (NCC) at a Commission facility located in Gettysburg, Pennsylvania. The Commission news release announcing the opening reported that the Call Center "provides simple, one stop shopping for information about FCC rules and policies." Since its introduction in 1996, the Call Center has seen a tremendous increase in the volume of activity and the degree to which automated tools are used to respond to customer inquiries. Initially, NCC consumer and information affairs specialists responded to customer inquiries and average monthly traffic was less than twenty thousand (20,000) calls. By March 1999, average monthly traffic (responses to customer inquiries) was exceeding sixty thousand (60,000) with monthly traffic occasionally exceeding eighty thousand (80,000) calls. In Fiscal Year (FY) 1998, the Commission reported that the Call Center responded to 1,070,448 calls. During the period that fieldwork was being performed on this audit, management control of the NCC was taken away from the now-defunct Compliance and Information Bureau and given to the newly created Consumer Information Bureau (CIB), and the NCC was renamed the Consumer Center. For purposes of reporting the results of our audit, we refer to the Consumer Center as the NCC or the "call center."

The ability of the Call Center to be responsive to customer inquiries and provide accurate, timely information is heavily reliant on automated systems. The objective of this audit was to examine the Call Center's automated computer system and the environment in which it operates, to ensure that adequate security safeguards exist to protect NCC data. To conduct this review, the OIG established a task order under our contract with the computer security firm of TWM Associates, Inc. (hereafter referred to as "TWM") to conduct an assessment of the current security posture of general computer controls utilized throughout the Call Center. TWM performed the audit of Call Center general computer controls in accordance with the General Accounting Office (GAO) Federal Information Systems Controls Audit Manual (FISCAM). The security requirements used as the basis of this audit were derived from Federal regulations and FCC policy. These regulations and policies included:

- Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources", dated February 8, 1996.

- FCC Instruction (FCCINST) 1479.1, entitled "FCC Computer Security Program", dated November 30, 1995.

- 18 USC §1030 Computer Fraud and Abuse Act

The audit was conducted in two phases. The objective of the survey phase was to identify previous audits and existing design, implementation, and operational documents that describe the business processes, organizations, and security policies associated with the NCC. The objective of the verification phase was to verify the security posture of the NCC in the areas of Security Program Planning and Management, Access Controls,

Application Software Development and Change Controls, System Software, Segregation of Duties, and Service Continuity.

The audit team noted that significant technical control and internal control improvements could be made to improve the overall security posture of the NCC. Many of the procedures performed and the resulting findings focus on plans, policies, and procedures in place to ensure that NCC systems are administered in a secure manner. The technology-based findings focus on the secure implementation and deployment of technology within the NCC systems. The combination of plans, policies, procedures and properly implemented technical controls are inextricably linked. The plans, policies, and procedures provide guidance to ensure that the technology utilized in the system provides a minimum threshold of security, while the technology controls implementation itself ensures that the security goals and objectives put forth by management are achieved.

Based on the audit procedures performed and the findings identified by the audit, NCC systems' general computer controls as implemented are not sufficient to meet minimum security requirements. Specifically, this audit uncovered one hundred three (103) findings, thirteen (13) of which were classified with a high level of risk, fifty-two (52) with a medium level of risk, and thirty-eight (38) with a low level of risk[1]. Several of these findings are associated with key control areas. For example, access controls (to include system access and physical security of the computer facilities) represented sixty-nine (69) of the one-hundred three (103) findings. Nine (9) of the access control findings were high risk, forty (40) were medium risk, and twenty (20) were low risk. The extent and interrelationship of these findings indicate an inadequate security posture.

A summary of the audit findings is included in the section of this report entitled "Audit Findings". Detailed audit findings are included in Appendix A of the report entitled "Detailed Findings and Recommendations." Because of the sensitive nature of the detailed findings, Appendix A is watermarked "Sensitive" and distribution of Appendix A will be limited to those persons with a need for the information. In addition, Appendix B includes the relevant sections of FCC Instruction 1479.1, Computer Security Program Directive, Office and Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, and Title 18 USC Section 1030, Computer Fraud and Abuse Act. These documents provided the criteria by which we assessed the adequacy of the Call Center's general controls.

On March 31, 2000, we provided a draft report to CIB summarizing the results of our review and requesting their comments on the reported findings. We received a response from the Bureau Chief on May 31, 2000 and additional information from the CIB System Security Office (CIB-SSO) on June 13, 2000. The Bureau concurred with all of the

---

1 Each finding was evaluated to determine its degree of exposure. A **high risk** rating is defined as a security risk extreme enough to cause on-going operational concerns in the event of an occurrence. A **medium risk** rating is defined as a security risk to cause moderate on-going operational annoyances, but it would not cause a business disruption in the event of an occurrence. A **low risk** rating is defined as a security risk to cause minimal on-going operational efficiency issues, but it would not cause a business disruption in the event of an occurrence; and/or an event that may disrupt operations but the likelihood of an occurrence to that extent is remote.

reported findings and is currently developing corrective action plans to address the findings. We have incorporated CIB comments into the detailed findings portion of the report contained in Appendix A. We will monitor the development of these action plans and will perform a follow-up audit to assess the effectiveness of the corrective actions in addressing the deficiencies.

AUDIT OBJECTIVES

The objective of this audit was to examine the NCC's automated computer system and the environment in which it operates, to ensure that adequate security safeguards exist to protect NCC data. Specifically, the audit assessed the general computer controls in the areas of:

- Security Program Planning and Management;
- Access Controls;
- Application Software Development and Change Controls;
- System software;
- Segregation of Duties; and
- Service Continuity.

AUDIT SCOPE

The audit was conducted in accordance with generally accepted auditing standards and *Government Auditing Standards* issued by the Comptroller General of the United States. Further, the audit reviewed NCC security characteristics to determine whether they are in accordance with federal regulation maintained in Office of Management and Budget (OMB) Circular A-130, following the general controls procedures outlined in the Federal Information Systems Controls Audit Manual (FISCAM) proscribed by the General Accounting Office (GAO).

During the period that fieldwork was being performed in this review, management control of the NCC was taken from the now defunct Compliance and Information Bureau and given to the newly created Consumer Information Bureau, and the NCC was renamed the Consumer Center. The scope of our audit did not include an assessment of the changes resulting from the reorganization or the effect the reorganization may have on the IT controls governing the Call Center. In any event, the findings indicate significant security concerns in the NCC computer controls environment which should be addressed by the new organization.

To perform this review, we established an audit team of OIG and TWM personnel. The team employed a comprehensive set of procedures to review the general controls currently employed by the NCC site. During the first phase of the audit, the audit team surveyed information on FCC policies, previous OIG or other regulatory audit reports and methodologies, and design, implementation and operational audit documents covering the NCC. As part of this effort the NCC OIG audit team focus was on the NCC

topology (high level) and network schematic (low level) of NCC connectivity, to include identification of hardware, routers, and software components.

Based on our analysis of the information gathered during the survey phase, the audit team designed the steps to be performed during the verification phase of the audit. The objective of the verification phase was to verify the security posture of the NCC in the areas of Security Program Planning and Management, Access Controls, Application Software Development and Change Controls, System Software, Segregation of Duties, and Service Continuity.

The audit team performed specific general controls procedures for each of the following areas of the FISCAM:

- Assessed the framework and continuing cycle of activity for risk management, development of security policies, and assignment of responsibilities for monitoring the adequacy of the NCC controls;

- Assessed the controls that limit or detect access to computer resources: data, programs, equipment, and facilities; examined the Call Center's automated computer systems by reviewing the NCC network architecture for security vulnerabilities, and determined whether security controls and features have been incorporated into the NCC network architecture;

- Assessed the controls for software development and change control;

- Assessed the controls for the prevention of development and/or modification of unauthorized program changes;

- Assessed the segregation of duties through review of policies, procedures, and organizational structure; and

- Assessed controls to ensure continued operations without interruption.

The FISCAM procedures were completed through a combination of manual and automated procedures. Manual procedures consisted of interviews, review of documents, review of security settings measured against vendor recommended settings and good business practices, and review of processes performed. Automated procedures consisted of the use of proprietary platform security review software tools and commercially available scanning tools.

In addition to the FISCAM audit procedures, the security requirements used as the basis of this audit were derived from Federal regulations and FCC policy. These regulations and policies included:

- Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources", dated February 8, 1996.

- FCC Instruction (FCCINST) 1479.1, entitled "FCC Computer Security Program", dated November 30, 1995.

- 18 USC §1030 Computer Fraud and Abuse Act.

The sections of these regulations and policies that were relevant to this audit are included in Appendix B.

The audit took place from October 1999 through January 2000 and was conducted primarily at the FCC NCC site located at 1270 Fairfield Road in Gettysburg, Pennsylvania.

BACKGROUND

On October 21, 1996, the FCC opened the Call Center at a Commission facility located in Gettysburg, Pennsylvania. The Commission news release announcing the opening reported that the Call Center "provides simple, one stop shopping for information about FCC rules and policies." Since its introduction in 1996, the Call Center has seen a tremendous increase in the volume of activity and the degree to which automated tools are used to respond to customer inquiries. Initially, NCC consumer and information affairs specialists responded to customer inquiries and average monthly traffic was less than twenty thousand (20,000) calls. By March 1999, average monthly traffic (responses to customer inquiries) was exceeding sixty thousand (60,000) with monthly traffic occasionally exceeding eighty thousand (80,000) calls. In Fiscal Year (FY) 1998, the Commission reported that the Call Center responded to 1,070,448 calls. During the period that fieldwork was being performed on this audit, management control of the NCC was taken away from the now-defunct Compliance and Information Bureau and given to the newly created Consumer Information Bureau (CIB), and the NCC was renamed the Consumer Center. For purposes of reporting the results of our audit, we refer to the Consumer Center as the NCC or the "call center."

The ability of the Call Center to be responsive to customer inquiries and provide accurate, timely information is heavily reliant on automated systems. The NCC mission is supported by three (3) primary information systems. These systems, the Automatic Call Director system, the Integrated Voice Response System (IVRS), and the Expert Advisor system, support all aspects of Call Center operations. Two (2) of the information systems address Call Center workload management and call distribution requirements. The Automatic Call Director system takes incoming calls and distributes calls among the consumer and information affairs specialists and the Integrated Voice Response System (IVRS), added in 1998, enhances Call Center traffic management. The third system, the Expert Advisor System, support Call Center requirements for providing timely and accurate information to customers on a wide range of topics.

The NCC site consists of three (3) networks separated by infrastructure components. There is an inside network consisting of the main portion of the NCC application servers.

In addition, there is a dial-in network that is connected to the inside network by a CISCO 7507 router. The Dial-In network then connects to the telephone company circuit network. The Auctions site employs a Demilitarized Zone (DMZ) connected to the Internet through a CISCO PIX firewall. The DMZ is connected to the inside network through a combination of three (3) firewalls. The NCC network is connected through the Auction site router to the inside network, and thus receives additional protection from the DMZ and the three (3) firewalls. The NCC relies upon the Commission's Information Technology Center (ITC) for Intrusion Detection through an outsource agreement with Bell Atlantic. Bell Atlantic provides reports regularly and on demand for intrusion events such as port scans, patterns of known attacks, repetitive access denials and other signs of possible automated or manual attacks.

AUDIT FINDINGS

This audit was performed to assess the Call Center's general computer controls for their information technology environment, ensuring that the systems are adequately secured. The audit includes recommendations to mitigate the possibility of the system being compromised. The audit recognized both strengths and weaknesses of the technical and procedural internal controls currently employed. The Call Center has implemented controls with their limited resources in some areas, but the overall security posture can be improved. The implementation of the technical control recommendations should result in the most immediate improvement of the NCC security posture. Further, the achievement of a proper segregation of duties and implementation of adequate technical training should also assist in achieving the minimum security requirements contained in the OMB Circular A-130 and FISCAM guidance.

Based on the procedures performed in accordance with FISCAM guidance, we have concluded that there is insufficient implementation of general computer controls. While the NCC gains some general computer controls implementation from the overall FCC infrastructure, sufficient general controls do not exist at the NCC level to ensure protection of NCC resources.

The audit team noted that significant technical control and internal control improvements could be made to improve the overall security posture of the NCC. Many of the procedures performed and the resulting findings focus on plans, policies, and procedures in place to ensure that NCC systems are administered in a secure manner. The technology-based findings focus on the secure implementation and deployment of technology within the NCC systems. The combination of plans, policies, procedures and properly implemented technical controls are inextricably linked. The plans, policies, and procedures provide guidance to ensure that the technology utilized in the system provides a minimum threshold of security, while the technology controls implementation itself ensures that the security goals and objectives put forth by management are achieved.

This audit uncovered one hundred three (103) findings, thirteen (13) of which were classified with a high level of risk, fifty-two (52) with a medium level of risk, and thirty-eight (38) with a low level of risk. Several of these findings can be identified with key

control areas. For example, access controls (to include system access and physical security of the computer facilities) represented sixty-nine (69) of the findings, nine (9) of which were high risk, forty (40) were medium risk, and twenty (20) were low risk. A less extensive example is in the area of network controls, which includes overall risk management and system software controls. Our audit disclosed 14 findings related to network controls, of which one (1) finding was high risk, ten (10) were medium risk, and three (3) were low risk. Each of these findings taken individually may or may not represent a significant security risk, however, the number of findings taken together represents insufficient network controls are in place. The extent and interrelationship of these findings indicate an inadequate security posture.

Based on the procedures performed and the extent of the resultant findings, NCC systems' implemented general controls are not sufficient to meet the minimum security requirements as tested with the FISCAM procedures. However, implementation of the audit recommendations can bring the NCC systems' security posture in line with FISCAM and OMB Circular A-130 security requirements.

We provided a draft report to the Consumer Information Bureau (CIB) on March 31, 2000 and requested their comments on the findings. We received a response from the Bureau Chief on May 31, 2000 and additional information from the CIB System Security Office (CIB-SSO) on June 13, 2000. The Bureau concurs with all of the observations being reported and is currently developing corrective action plans to address the findings. The corrective action plans are being coordinated with all Bureaus/Offices that are impacted by the findings, to include:

- The Information Technology Center Applications Integration Group (ITC-AIG);
- The Wireless Telecommunications Bureau (WTB);
- The CIB Assistant Bureau Chief of Management (CIB-ABCM); and
- The Information Technology Center Network Development Group (ITC-NDG).

OIG will monitor the development of these action plans and will perform a follow-up audit to assess the effectiveness of the corrective actions in addressing the deficiencies.

APPENDIX A

Detailed Findings and Recommendations

OVERVIEW

The General Accounting Office (GAO) Federal Information System Controls Audit Manual (FISCAM) is primarily designed for evaluations of general and application controls over financial information systems that support agency business operations. However, it is also used in evaluating the general and application controls over agency program information systems, as called for in the Government Auditing Standards issued by the Comptroller General.

The FISCAM areas reviewed in this audit and further discussion of the audit procedures performed to evaluate the FISCAM objectives are as follows:

1. Security Programming and Management

Security programming and management controls govern procedures for developing and updating risk management plans, developing security policies, assigning responsibilities, and monitoring the adequacy of computer-related controls. To evaluate the security programming and management controls, the audit team interviewed individuals regarding security policies, hiring, termination and transfer policies, and training. In addition, employee job descriptions and employee files were reviewed as part of these procedures.

During our review of security programming and management controls, we identified findings regarding controls over the establishment of formal policies and procedures, where policies and procedures existed, the need for updating policies, and procedures to reflect the current operating environment.

2. Access Controls

Access controls focus on the controls that limit or detect access to computer resources (both system access and physical security of computer facilities) to protect resources against unauthorized modification, loss, and disclosure. To evaluate the access controls, the audit team analyzed the servers and network devices used in the NCC systems. The servers and devices include UNIX, Windows NT, and Novell system software, Sybase database software, Definity Audix and PBX devices, and CISCO router security settings. In addition, the Internet Protocol (IP) addresses linked to NCC were scanned to determine if unnecessary services were present. The audit team used the FISCAM as well as proprietary technology-specific review procedures that are based on vendor recommendations and good business practices, automated security review software, and commercially-available scanning tools. Additionally, the team assessed the physical security of the facilities by reviewing physical security requirements observing the NCC's implementation of security measures.

A significant number of our findings were due to the installation of system and database software without changing default settings and a lack of consideration for the use of system audit capabilities. In addition, numerous weaknesses in physical security were identified.

3. Application Software Development and Change Controls

Application software development and change controls are designed to prevent unauthorized programs or modifications to an existing program from being implemented. The scope of our review of application software development and change controls included reviewing the informal program change controls.

Our audit found that, while informal program change control procedures could be identified for one of the NCC applications (Expert Advisor), the procedures are not formally documented and program change tracking is manual, and thus subject to error or untimely updates. The other applications were even less formal in the program change control process.

4. System Software

System software controls focus on the controls that limit and monitor access to the system software programs and sensitive files that control the NCC's computer hardware and secure applications supported by the system. To evaluate system software controls, we reviewed the development, testing, and implementation of system software such as version updates for UNIX, Windows NT, Sybase, Novell, and CISCO router software. The audit team also requested documentation for evidence of up-to-date policies and procedures for monitoring system utilities, controlling system changes, and monitoring programmers' activities.

Our audit of system software controls disclosed that, while procedures may be used in the development, testing, and implementation of system software changes, formal procedures and support for system software changes specific to NCC could not be provided during the course of this audit. Our recommendations in this control area include suggestions for establishing and improving current policies and procedures, in addition to technology-specific improvements.

5. Segregation of Duties

Segregation of duties relates to controls that ensure that no one individual could control key aspects of FCC's computer-related operations and thereby conduct unauthorized operations or gain unauthorized access to records or assets. Our review of segregation of duties included an examination of the policies, procedures and organizational structure of the NCC. We also requested documentation describing employee responsibilities, duties, and formal job descriptions, and interviewed personnel and reviewed documentation describing job rotation, vacation, staff monitoring, and manager reviews. Personnel records were also reviewed.

Our audit identified a lack of documented policies and the need for further segregation of duties among operational functions, program development functions, and system administration functions.

6. Service Continuity

Service continuity controls are designed to ensure that service continuity is maintained when unexpected events occur; that is, critical operations continue without interruption or are promptly resumed, and critical and sensitive data are protected. A physical security audit was also performed for the NCC facility and surrounding area. During our evaluation of service continuity practices, we requested documentation of contingency and disaster recovery plans and the results of testing those plans.

Formal contingency and disaster recovery plans for NCC were not provided during the course of the audit. While written documentation did exist for one of the applications (Expert Advisor), formal plans did not exist for other applications or for telecommunications and infrastructure processes. In addition, no testing of contingency or disaster recovery plans had been performed.

DETAILED FINDINGS AND RECOMMENDATIONS

The audit uncovered 103 findings encompassing all FISCAM review areas. As part of the review, the audit team evaluated each finding to determine its degree of exposure based on the following exposure ratings:

> **High**: The security risk is extreme enough to cause on-going operational concerns in the event of an occurrence.
>
> **Medium**: The security risk is moderate to cause on-going operational annoyances, but would not cause a business disruption in the event of an occurrence.
>
> **Low**: The security risk is minimal to cause on-going operational efficiency issues, but would not cause a business disruption in the event of an occurrence; and/or an event that may disrupt operations but the likelihood of an occurrence to that extent is remote.

Using these exposure ratings, the breakdown of findings is as follows:

Exposure Rating	Number of Findings
High	13
Medium	52
Low	38
Total	103

Contained in the following pages are the detailed NCC findings and recommendations. They are presented by order of the assigned High, Medium, or Low risk factors. The primary criteria used for the findings was the FCC Directive, FCC INST 1479.1 which is the FCC's implementation of OMB-A130, on which the FISCAM procedures are based.

APPENDIX B

Audit Criteria

FCC Instruction 1479.1 Computer Security Program Directive, dated November 30, 1995

The purpose of FCC Instruction 1479.1 Computer Security Program Directive, dated November 30, 1995 is as follows:

Purpose. This directive establishes policy and assigns responsibilities for assuring that there are adequate levels of protection for all FCC computer systems (Personal Computers (PCs), Local Area Networks (LAN), the FCC Network, and applications and databases), and information created, stored, or processed, therein. This document addresses issues relating to all aspects of computer systems security, including issues concerning day-to-day security safeguards, business continuity, system accessibility, software licensing, and administrative precautions which can be taken by users of the FCC computer systems and those who manage them.

Section 6.c.3 of FCC Instruction 1479.1 states:

6. Responsibilities.

   c. *AMD-IM, Computer Security Officer*

      3. Coordinate with Functional Managers and AMD-IM Network Management Division staff to provide oversight on the process of conducting risk analyses and security test and evaluations (ST&E), the preparation of Continuity of Operations Plans (COOP) and security plans, and the certification of sensitive FCC information systems;

Section 6.d.1 of FCC Instruction 1479.1 states:

   d. *AMD-IM, Network Management Division*

   AMD-IM, Network Management Division (NMD) will assist with the implementation of this directive and its policy and standards. The Computer Security Officer will coordinate with NMD to assist FCC users in the development of procedures that conform to this directive. Further, NMD shall develop and implement appropriate administrative and technical procedures to conform with this directive, and other related Federal regulations, and FCC directives and policies. To support this effort, NMD shall:

      1. Coordinate with the Computer Security Officer to establish and maintain procedures which will ensure the security and integrity of respective FCC computer systems. Procedures should provide adequate safeguards for

processing and storing sensitive data and limiting access to systems, therein;

Section 6.d.6 of FCC Instruction 1479.1 states:

6. Coordinate with the Computer Security Officer to provide oversight on the development and testing of security plans and contingency plans, and provide oversight on the conduct of risk analyses of FCC sensitive systems;

Section 6.e.1 of FCC Instruction 1479.1 states:

e. *AMD-IM, Computer Applications Division*

AMD-IM, Computer Applications Division (CAD) will assist with the implementation of this directive and its policy and standards. The Computer Security Officer will coordinate with CAD to assist FCC users in the development of procedures relating to CAD functions that conform to this directive. To support this effort, CAD shall:

1. Provide FCC user assistance to develop application(s) and database security and contingency plans, and as appropriate conduct application risk analyses; and

---

Section 6.h.1 of FCC Instruction 1479.1 states:

h. *Security Operations Staff, AMD-O, Operations Management & Services Division (Security Operations Staff)*

The Security Operations Staff/Personnel Security Office are responsible for:

1. Arranging background checks for FCC users in sensitive computer-related positions as required by applicable regulations; and

---

Section 6.k.5-6 of FCC Instruction 1479.1 states:

k. *Authorized PC/LAN System Users.*

An informed, educated, and alert user is a crucial factor in ensuring the security of FCC's computer systems and valuable information resources. To support this effort, users shall:

5. Recognize the accountability for all activity taking place with the assigned userID and associated account;

6. Change computer system passwords every 180 days;

Section 7.a of FCC Instruction 1479.1 states:

7. System Access Controls.

a. User Identification and Authentication. User identification and authentication occurs whenever a computer session is established. To support this process, each user must use a unique userID/password. The following standards should be followed by FCC users:

- Each user must have a unique userID to access FCC computer systems. Under normal circumstances, users should not share their userID or password with anyone. In emergency situations where the user must provide the Help Desk or their supervisor access to their account, the user should change the password immediately upon the next login;

- AMD-IM, Network Administrators should review audit logs to determine if there have been repeated unsuccessful attempts to login to FCC computer systems;

- Training and maintenance userIDs should be administered through a secure and documented process. These userIDs must be rendered inactive when not being used for training or maintenance tasks;

- In general, userIDs should not be permitted to initiate multiple concurrent logins to access FCC computer systems. Exceptions are considered on a case-by-case basis;

- If using automatic login scripts for system access, the script must not contain the user's login password;

- Guest userIDs should be limited to remote printing capabilities for authorized users with an authorized userID account on FCC computer systems; and

- Guest userID access to FCC computer systems via remote dial-in must be prohibited.

Section 7.b of FCC Instruction 1479.1 states:

b. Password Controls. Passwords are an accepted method of authentication at the FCC and play a vital role in securing access to any FCC computer system. Passwords should be stored with one-way encryption, where only the user has the ability to know the password. Users forgetting their password and requiring the password to be reset should contact the Help Desk. The following are standards on password use for access to FCC computer systems:

   - Users should select strong passwords (i.e., not the same or reverse as the userID, not the users name or initials, not words easily found in a dictionary, etc.);

   - Under all circumstances, a unique userID and password, only known by the user, must be used to access FCC computer systems;

   - User should change passwords periodically, but at a minimum of every 180 days, as required by the system;

   - Use passwords with a minimum length of six characters (alpha/numeric characters are preferred);

   - Users should not write passwords down, but should be easily remembered;

   - When a password has been, or is believed to have been compromised, a new password should be established and the user should contact their supervisor or COTR and the Help Desk; and

   - AMD-IM, Network Administrators should set the userID to be revoked if a password attempt threshold of three failed login attempts is exceeded. When the threshold is reached, the user must contact the Help Desk to have the account reset.

Section 7.c of FCC Instruction 1479.1 states:

c. Application/Data Base Controls. Controls should be implemented to assure the integrity of FCC computer systems. These controls should make certain that information and resources correctly reflect the expected and understood configuration and composition of data, applications, and programs operating on FCC computer systems.

- FCC users should be restricted to only those resources required for the efficient completion of their job responsibilities;
- Access control software and/or network operating system security should be kept current and controls limiting user access to sensitive data, applications, and programs should be in place;
- When technically possible, logs should be maintained to monitor system usage, and used to establish accountability for changes to data and programs;
- Ensure that software license agreements are adhered to, and as required, ensure that appropriate software metering mechanisms are in place and used to monitor software use;
- Ensure that network applications installed on FCC system servers are designated as execute-only or read-only, as necessary; and
- Updates and changes to applications/databases should be thoroughly tested to prevent unintentional access capabilities.

Section 9 of FCC Instruction 1479.1 states:

9. Awareness, Training, and Education. The Computer Security Act of 1987, P.L. 100-235, was enacted to improve the security and privacy of sensitive information in Federal computer systems. As one way of meeting that goal, the law requires that "each agency shall provide for the mandatory periodic training in computer security awareness and accepted computer practices of all employees who are involved with the management, use, or operation of each federal computer system within or under the supervision of that agency."

Section 12.c of FCC Instruction 1479.1 states:

12. Software Management. The use of software on FCC computers that is not properly licensed is not permitted. In addition, software that you may have purchased must be

pre-authorized for installation on your local drive (C:). In addition, users are not authorized to place software, that has been licensed for individual use, on any shared drive.

c. Copying Software from FCC Computer Systems. Users of FCC computer resources are not authorized to copy software from the system. Most software installed on FCC computer systems is designated as execute-only or read-only, as necessary. Users requiring a copy of the software loaded on FCC computer systems for a remote PC should contact the Help Desk for assistance.

Section 13 of FCC Instruction 1479.1 states:

13. Computer Virus Prevention and Management.

- Use an up-to-date, FCC approved anti-virus program. AMD-IM, NMD will ensure that the most current version of the software selected for use at the Commission is available for use. Users should scan computer drives and check diskettes prior to use, including those received from other employees, contractors, or outside sources.

Section 14.a of FCC Instruction 1479.1 states:

14. Physical Security and Computer Equipment Handling. The offices and work areas where FCC computer systems are located must be physically secured when unattended. Adequate controls should be employed consistent with the value, exposure and sensitivity of the information and equipment that is to be protected. Although the value of a computer can be significant, the value or importance of the information, can be far greater. It is recommended that management establish controls that include any or all of the following:

a. Area Access Controls. FCC users have a responsibility to create and maintain a secure work environment, and to protect the computer assets used to fulfill business activities. Access to offices and work areas, where FCC information, and computer resources are located, should be controlled in a manner that permits access only to authorized persons. In addition, it is strongly recommended that each user activate the system provided Screen Saver and associated password on their PC. The use of the Screen Saver with password will ensure that while the PC is unattended, no one but the person knowing the password can gain access to the system via the user's account.

The controls needed in FCC business areas depend upon the information resources housed in the area and the level of exposure. Managers should implement the following controls to protect information assets under their control:

- Ensure that FCC users understand their responsibility for maintaining a secure and safe work area. Furthermore, each individual should take reasonable measures to assure the security and safekeeping of the computer systems and information being used; and/or

- Ensure that access to areas housing computer resources are controlled. Persons authorized to access area should be FCC users, or visitor(s) accompanied by FCC users.

Section 14.b of FCC Instruction 1479.1 states:

b. Preventing Hardware Theft. Information and computer equipment must be protected against theft. Loss of certain information, if not properly backed-up, can require significant effort to recreate. Significant repercussions may ensue if the lost information is subject to FOIA compliance. It is recommended that Bureaus/Offices select and implement security controls that employ any or all of the following measures:

   - Only authorized FCC users should have access to areas where computer resources, processing sensitive or mission critical FCC information, are housed. Authorization to controlled areas should be granted, and removed when applicable, on a "need to access basis";

   - Work and storage areas housing computer resources should have locked doors, cabinets, or desks, in use. When computer hardware storing sensitive or mission critical information is not secured by a locked door, it should be secured with equipment enclosures and/or lock-down devices. Accessory equipment like modems and external disk drives should be secured in a similar fashion;

   - Sensitive correspondence, reports and spreadsheets in hard-copy form or on magnetic media should be stored in locked containers, desks or file cabinets; and

   - FCC users should provide visual coverage of computer resources during business hours if the resources are not in a lockable area.

Section 14.f of FCC Instruction 1479.1 states:

f. Environmental Protection. PCs are sensitive to the quality of electrical power. As a result, surge protectors should be used to regulate electrical current and absorb abnormal electrical levels. Drinking and eating should be discouraged in the immediate vicinity of PCs and related peripherals.

   The Computer Room and hub rooms contain, in most cases, the highest concentration of support equipment and information used at the FCC. Sufficient suppression systems must be installed to mitigate the possibility of power spikes for incoming power supplies. In addition, battery back-up via an uninterruptable power supplies (UPS) or similar process must be installed to provide system(s) server and peripherals support in the event of a power failure.

Section 15.b of FCC Instruction 1479.1 states:

15. Computer System Business Recovery.

    b. Application and Data Back-Ups. To be usable, copies of electronic media must be made accurately, regularly, and consistently. AMD-IM, NMD shall ensure that adequate network back-ups are maintained, including files created using the standard office automation software suite. Precautions should be made to ensure that the type of media used does not become faulty over time using a periodic test scenario. Functional Managers shall ensure that adequate back-ups are made of applications/databases, and data within their control and which are stored on FCC computer systems.

The off-site location should provide similar protection to environmental threats and physical access, as do that of the Computer Room, and hub rooms.

Section 16 of FCC Instruction 1479.1 states:

16. Sensitive Data/Application Management. Oversight for computer data and associated resources resides with the Bureau/Office requesting the purchase of the peripheral(s) or development of the application and/or data. Bureau Chiefs and Office Directors should assign ownership to an appropriate Functional Manager within a Division, Branch, or any functional entity within that Bureau/Office. Management responsibilities should not be construed as replacing or diluting the Computer Security Officer's or AMD-IM's responsibilities for compliance with computer security requirements.

    Designated Functional Managers of FCC's computer system/applications should:

- Acknowledge responsibility of resources and identify those containing or processing sensitive data;
- Coordinate with the Computer Security Officer to develop protection controls;
- Authorize access to computer resources under their control;
- Educate managers and users on control and protection requirements for computer systems and information;
- Monitor compliance with established security FCC directives, Federal regulations and other applicable mandates, and periodically review control processes; and
- Ensure the conduct of risk analyses and the development of contingency plans.

Section 19 of FCC Instruction 1479.1 states:

19. Destruction of Sensitive Data. The useful life of every computer document should end with its destruction in a safe and secure manner. All forms of media (hard-copy, magnetic, etc.) containing sensitive data require a safeguarded means of destruction.

OMB Circular A-130 Management of Federal Information Resources, revised February 8, 1996

OMB Circular A-130, Section 5 states:

The Paperwork Reduction Act establishes a broad mandate for agencies to perform their information resources management activities in an efficient, effective, and economical manner. To assist agencies in an integrated approach to information resources management, the Act requires that the Director of OMB develop and implement uniform and consistent information resources management policies; oversee the development and promote the use of information management principles, standards, and guidelines; evaluate agency information resources management practices in order to determine their adequacy and efficiency; and determine compliance of such practices with the policies, principles, standards, and guidelines promulgated by the Director.

OMB Circular A-130, Section 7.n states:

n. Users of Federal information resources must have skills, knowledge, and training to manage information resources, enabling the Federal government to effectively serve the public through automated means.

OMB Circular A-130, Section 8.a.d states:

8. -- Policy:

a. Information Management Policy

4. Records Management. Agencies shall:

(d) Provide training and guidance as appropriate to all agency officials and employees and contractors regarding their Federal records management responsibilities.

OMB Circular A-130, Section 8.9.b.4.f states:

8. -- Policy:

9. Safeguards. Agencies shall:

b. Information Systems and Information Technology Management

4. Use of Information Resources

(f) Establish a level of security for all information systems that is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained in these information systems.

OMB Circular A-130, Section 8.a(c) states:

8. -- Policy:

a. Information Management Policy
(c) Agencies shall limit the sharing of information that identifies individuals or contains information to that which is legally authorized, and

impose appropriate conditions on use where a continuing obligation to ensure the confidentiality of the information exists.

Appendix III to OMB Circular No. A-130, Section A.3.b.2.a

A. -- Requirements.

3. -- Automated Information Security Programs.

b. Controls for Major Applications.

2) Application Security Plan.

a. Application Rules. Establish a set of rules concerning use of and behavior within the application.

Appendix III to OMB Circular No. A-130, Section B.a.2.c

B. -- Descriptive Information.

a. General Support Systems.

The following controls are required in all general support systems:

2. Security Plan.

c. Personnel Controls.

It has long been recognized that the greatest harm has come from authorized individuals engaged in improper activities, whether intentional or accidental. In every general support system, a number of technical, operational, and management controls are used to prevent and detect harm. Such controls include individual accountability, "least privilege," and separation of duties.

Separation of duties is the practice of dividing the steps in a critical function among different individuals. For example, one system programmer can create a critical piece of operating system code, while another authorizes its implementation. Such a control keeps a single individual from subverting a critical process.

Title 18 USC 1030

Title 18 USC Sec. 1030. Fraud and related activity in connection with computers, paragraph (a)(3)states:

- (a) Whoever –

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States.

(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.