Attachment 4

	FEDERAL COMMUNICATIONS COMMISSION Washington, DC 20554	FCC DIRECTIVE	
		FCCINST 1479.2	
	FCC DIRECTIVE	Effective Date: October 2, 2001	Expiration Date: October 2006

To: All Employees and Contractors

Subject: FCC Computer Security Program

1. 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, 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 and authentication, software licensing, and administrative precautions, which can be taken by users of the FCC computer systems and those who manage them.

2. AUTHORIZATION

This directive fulfills the requirements of Office of Management and Budget (OMB) Circular A-130, Appendix III, The Computer Security Act of 1987 (Public Law 100-235), Government Information Security Reform Act (Public Law 106-398) and other applicable guidelines and laws.

3. CANCELLATION

FCCINST 1479.1, FCC Computer Security Program Directive, dated November 30, 1995.

4. APPLICABILITY

The provisions of this directive apply to all FCC employees, including telecommuters, and contractors (herein referred to as FCC users) who use a computer system or access computer generated data to conduct business on behalf of the FCC. This directive discusses safeguard measures to be taken for computer related information systems processing or containing sensitive and Commission critical data. The directive should also be used as a minimum standard for safeguarding other non-sensitive information processed or stored on FCC computer equipment.

DISTRIBUTION: ALL EMPLOYEE	ORIGINATOR: Computer Security Information Technology Center Office of Managing Director

5. POLICY

With all FCC computer systems, users shall have no expectation of privacy. As described in the required banner displayed at each login to FCC computer network, use of FCC computer systems is for FCC authorized purposes only. Appropriate administrative, audit and investigative efforts may result from inappropriate system use. All information within FCC systems is subject to access by authorized FCC personnel at any time. Individual users have no privacy interest in such information. Additional system usage allowances are discussed under Section 11 and 12 on Internet and Email use. All related systems and information shall be secured to at least the minimum level of security defined in this and other related FCC directives. FCC users must *not* process or store national security classified information on FCC computer systems, unless specifically authorized by both the Security Officer (Security Operations Center) and the Computer Security Officer (Information Technology Center).

6. RESPONSIBILITIES

6.1. *Managing Director, FCC*

FCC's Managing Director shall designate a senior official to have the primary responsibility for managing the Commission's Computer Security Program.

6.2. *Chief Information Officer (CIO), Information Technology Center (ITC)*

The Chief Information Officer shall perform the following duties:

6.2.1. Assign and direct a person responsible for managing the FCC's Computer Security Program.

6.2.2. Evaluate and approve the resolution of issues related to computer security.

6.3. *Computer Security Officer, FCC*

The Computer Security Officer is responsible for establishing, maintaining, directing, and coordinating implementation of this directive and for assisting FCC management and other FCC users with the development of procedures conforming to this and other related directives. Further, the Computer Security Officer will ensure that appropriate technical and administrative safeguards are in place, and complied with, to ensure an adequate level of security for FCC computer systems. To support this effort, the Computer Security Officer shall:

6.3.1. Develop overall Commission-wide computer security objectives and goals and act as the FCC computer security focal point;

6.3.2. Ensure that FCC users are provided effective security awareness training and direction on computer system practices;

6.3.3. Coordinate with the ITC Network Development Group staff, Application Integration Group and the Operations Group to provide oversight on the

process of conducting risk analyses and computer security reviews, the preparation of Continuity of Operations Plans (COOP) and security plans, and the processes involved in the conduct of certification and accreditation of major FCC applications;

6.3.4. Coordinate with Bureaus/Offices to provide oversight to conduct audits of computer-based programs to include periodic security inspections, and/or reviews of data in computer files to ensure compliance with this directive, and related Federal regulations and mandates;

6.3.5. Support FCC users with problems related to the security of FCC computer systems, and information stored therein;

6.3.6. Review incidents in which security lapses/breaches have occurred, prepare reports documenting specific events that lead up to the security breakdown(s), and recommend improvements for preventing future security lapses/breaches.

6.3.7. As requested by the Inspector General, assist on investigative matters, when relating to computer security;

6.3.8. Coordinate with Performance Evaluation and Records Management (PERM) to ensure compliance with the Freedom of Information Act (FOIA) and the Privacy Act of 1974 (PA), when requests pertain to information stored on the FCC network, or components therein;

6.3.9. Certify, as appropriate, that all sensitive FCC computer systems and associated security safeguards comply with this directive, Federal regulations, and related mandates prior to implementation in a production processing environment;

6.3.10. Manage the ITC Computer Incident Response Teams (CIRT);

6.3.11. Act as the Commission's focal point for computer security related advice.

6.4. *ITC, Operations Group*

The Operations Group (OG) will assist with the implementation of this directive and its policy and standards. To support this effort, OG shall:

6.4.1. 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.

6.4.2. Document event(s), and immediately notify the Computer Security Officer, whenever a known or possible breach of computer security occurs.

6.4.3. Take all reasonable steps to ensure that information processed or stored on FCC computer systems is kept secured while on the FCC network.

6.4.4. Ensure that all file server system management account passwords are changed at a minimum of every 90 days, or more frequently as required, and that passwords are provided only to persons with a bona fide need-to-know.

6.4.5. Establish written file and database server backup policies and procedures and ensure that they are followed.

6.4.6. Periodically review to ensure that only authorized software is installed on FCC computer system servers.

6.5. *ITC, Network Development Group*

ITC Network Development Group (NDG) will assist with the implementation of this directive and its policy and standards. To support this effort, NDG shall:

6.5.1. Develop and implement appropriate administrative and technical procedures to conform with this directive, and other related Federal regulations, and FCC directives and policies;

6.5.2. Compile and maintain a FCC computer system topology which clearly illustrates the entire network, including server locations, communication links, firewalls, and all other related network components maintained by the ITC;

6.5.3. Ensure that all system routers and firewall passwords are changed at a minimum of every 90 days, or more frequently as required, and that passwords are provided only to persons with a bona fide need-to-know;

6.5.4. Coordinate with the Computer Security Officer in the development and testing of contingency plans, and provide assistance on the conduct of network risk analyses;

6.5.5. Identify and recommend security solutions and safeguards for use on the FCC Network in order to avert or minimize potential security vulnerabilities;

6.5.6. Ensure that system audit logs and other available system management reports are accumulated and reviewed. Activities that show potential misuse should be forwarded to the Computer Security Officer for consideration.

6.5.7. Responsible for operation of ITC-managed firewalls, routers, and other network devices, and implementing security policies on firewalls and ITC-managed routers.

6.5.8. Ensure the integrity and security of ITC-managed firewalls and routers.

6.6. *ITC, Applications Integration Group*

ITC, Applications Integration Group (AIG) will assist with the implementation of this directive and its policy and standards. To support this effort, AIG shall:

6.6.1. Provide Bureaus and Offices assistance to develop application(s) and database that comply with this directive and other related federal mandates and policies.

6.6.2. Provide assistance to the Computer Security Officer to ensure that appropriate security reviews are conducted on FCC applications prior to being utilized in a production environment.

6.6.3. Ensure the security and integrity of UNIX and other production servers, databases and Internet application servers under AIG control.

6.6.4. Configure UNIX systems to meet security requirements.

6.6.5. Periodically review UNIX and other production systems to verify compliance with security requirements and fix any discrepancies.

6.7. *Bureau/Office Application Custodians/Managers*

Application Custodians/Managers are those Bureau/Office representatives who have the responsibility to manage respective sensitive and mission critical applications, databases, and/or information systems. (Note: ITC, Operations Group is considered the Application Manager for all general support systems.) Application Managers should comply with and implement the policies, standards and goals of this directive. They are also responsible for ensuring the development, administration, monitoring, and enforcement of internal controls, application security plans and continuity of operations plans, and incident reporting processes. Bureau/Office Custodians/Managers should contact the Computer Security Officer for technical support in the development and implementation of their policies, standards, and goals, as needed. To support the effort, Bureau/Office Managers shall:

6.7.1. Identify sensitive and mission critical systems, applications and databases, and files within their functional control.

6.7.2. Ensure that respective computer systems are used exclusively by authorized FCC users for the performance of official Commission business and that equipment is secured to prevent unauthorized use.

6.7.3. Ensure that sensitive and Privacy Act data are only released outside of the Commission, with the approval of the Performance Evaluation and Records Management (PERM), Privacy Act Officer.

6.7.4. Monitor user requirements to ensure that only those system access privileges are granted to perform current job responsibilities.

6.7.5. Ensure that respective computers systems follow the system backups policy (see Section 17.2)

6.7.6. Assist in the development of the Security Plan for the respective Major Application.

6.7.7. Work with Computer Security Officer to ensure that required level of computer security is put in place for each application, including contacting the Computer Security Officer at the appropriate points in the Systems Development Life Cycle (SDLC).

6.7.8. Report any security incidents to the Computer Security Officer.

6.7.9. Monitor respective systems for potential misuse and security threats.

6.7.10. Perform a review of user access privileges every 6 months.

6.8. *OMD, Performance Evaluation and Records Management*

The OMD, Performance Evaluation and Records Management (PERM) is responsible for ensuring that information safeguards mandated by the Freedom of Information Act (FOIA) and Privacy Act of 1974 (PA) are implemented and maintained across all FCC computer system platforms. To support this effort, PERM shall:

6.8.1. Determine the disclosure eligibility of data maintained on FCC computer systems based on FOIA and PA guidelines.

6.9. *Security Operations Center, Administrative Operations*

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

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

6.9.2. Ensuring adequate physical security for locations containing FCC computer and communications devices used to support the FCC computer system function;

6.9.3. Granting badge access to key FCC and ITC spaces based on a need-to-access criterion.

6.10. *Contracting Officer*

The FCC Contracting Officer shall ensure that qualified persons are assigned as Contracting Officers Technical Representatives (COTRs) for each task involving the management, development, or modification of FCC computer systems and information, therein.

Ensure that each Statement of Work (SOW) and task order comply with this directive and other related FCC and federal mandates and that all SOWs issued on behalf of the FCC include criteria to require compliance with this directive and related FCC and federal mandates.

6.11. *Contracting Officers Technical Representative (COTRs)*

COTRs shall:

6.11.1. Ensure that each Statement of Work (SOW) regarding computer systems and information solicitations contain appropriate language to ensure compliance with this directive and related FCC and federal mandates.

6.11.2. As deemed necessary, select an on-site Contractor Representative (to fill the role of Contractor Security Representative) who shall:

- Coordinate all computer system security procedures through the COTR.
- Ensure compliance with FCC's computer security directive, and related Federal regulations and mandates.
- Maintain a current list of names and telephone numbers for on-site/off-site contractors working on FCC contracts, which require access to FCC computer systems. In addition, ensure that a copy of each listing is provided to the Computer Security Officer.

6.12. *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 sensitive information resources. To support this effort, users shall:

6.12.1. Be aware of, and understand responsibilities to comply with this and related FCC directives.

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

6.12.3. Use FCC computer system resources only for lawful and authorized FCC business purposes, and access FCC computer systems and information only when a bona-fide business purpose exists.

6.12.4. Ensure that computers *are not* used to generate or send harassing or slurring messages, or similar graphical images.

6.12.5. Change passwords on assigned accounts every 180 days, at a minimum.

6.12.6. Use a password protected Screen Saver when leaving a logged-in workstation unattended.

6.12.7. Comply with safeguards, policies, and procedures that prevent unintentional or deliberate access to FCC computer systems by unauthorized persons.

6.12.8. Comply with the terms of software licenses and only install licensed software that is authorized for use at the FCC (see 14.1. Installing Non-FCC Standard Software on FCC Computers.) In addition, *do not* install or use game software on FCC computer systems.

6.12.9. Ensure that appropriate forms are completed and submitted pertaining to FCC computer systems access and use of resources, including: FCC Computer System Security Acknowledgement, Form A-201 (attached), used as Rules of Behavior to verify users obligation to secure the Commission's computer system and data; FCC Computer System Personally-Owned Software Certification, Form A-202 (attached), used to identify properly licensed personal software to be installed on a particular PC; and FCC Computer System Separation Clearance, Form A-203 (attached), used to announce the user's intention to relinquish computer systems access rights.

6.12.10. Promptly report known or suspected unauthorized use of computer resources, disclosure of user ID's and/or passwords to persons other than the assigned individual, or violations of this directive to the Computer Security Officer.

6.12.11. Attend mandatory FCC Computer Security Awareness Training as announced by the Computer Security Officer.

6.12.12. User shall not reconfigure desktop security settings without approval from the Computer Security Officer.

7. SYSTEM ACCESS CONTROLS

7.1. 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 Computer Resource Center (CRC) or their supervisor access to their account, the user should change the password immediately upon the next login.

- ITC System 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 unusable when not being used for training or maintenance tasks.

- In general, userIDs are not permitted to initiate multiple concurrent logins to access FCC computer systems. Exceptions are considered on a case-by-case basis, as approved by the Computer Security Officer.

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

7.2. 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. 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 user's name or initials, not words easily found in a dictionary, etc.).

- Users forgetting their password and requiring the password to be reset, will report to the Computer Resource Center (CRC) and show their badge for proper identification, prior to the CRC resetting their password.

- Remote users forgetting their password and requiring the password to be reset will call the CRC and provide appropriate identification (e.g. badge number, or other previously determined identification (e.g. pass phrase, special identifier, etc.)) to the CRC, prior to the CRC resetting their password.

- Use passwords with a minimum length of six characters (Using a password with a combination of alphanumeric and special characters is preferred, i.e. b4time%).

- 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 respective system.

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

- Users must run a password protected Screen Saver when leaving a workstation unattended.

- When a password has been, or is believed to have been compromised, a new password should be established and the user should immediately contact their supervisor or COTR and the Computer Security Officer.

- ITC System Administrators are required to set userID to be revoked if a password attempt threshold of three failed login attempts is exceeded. When the threshold is reached, account should be locked from access and scheduled to reset after 15 minutes.

7.3. Application/Data Base Controls. Controls should be implemented to ensure 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 application systems and data required for the efficient completion of their job responsibilities. The application custodian should perform a review of user access privileges every 6 months.

- 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 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.

- Updates and changes to applications/databases should be thoroughly tested, prior to the deployment in a FCC production environment, to prevent unintentional access capabilities.

8. INFORMATION SYSTEM ACCESS CONTROLS

8.1. Obtaining System(s) Access. The Computer Resource Center staff and the Computer Security Officer have established procedures, which, in conjunction with appropriate request forms, will allow personnel to access FCC computer system resources. Each user profile and access authorization must be supported by appropriate request forms. It is vital to the security of FCC computer systems that users only request access to data and systems for which a need-to-access exists. The FCC Computer System Security Acknowledgement, Form A-201 (attached and available on the intranet), must be properly completed and submitted to the CRC to obtain system(s) access.

FCC users can acquire forms and instructions by contacting the Computer Resource Center. The Bureau/Office Assistants for Management and/or Computer Resource Center (CRC) can also assist users in determining the type of access required and in completing forms.

8.2. Modifying System(s) Access. One important aspect of managing computer systems is to ensure that user privileges are kept up-to-date. At various times, a user may require modified systems access to perform position functions. As access requirements change, users must complete and submit the FCC Computer System Access Request form to the CRC for appropriate action.

8.3. Temporarily Suspending a Users Access. Periodically users may not require access to FCC computer systems (i.e., maternity/paternity leave, extended leave without pay, extended sick leave, etc.). In these situations, users or their supervisor, should notify their Bureau/Office Assistant for Management and the CRC to have their account temporarily suspended. This process is easily accomplished by submitting a priority electronic mail (email) message to the CRC with a courtesy copy to the Computer Security Officer. When the user returns to duty, the access can easily be reactivated by contacting the CRC. This process will ensure that unused access rights to the respective system are secured until the rightful user returns.

8.4. Removing System(s) Access. Prior to employment termination, each FCC user working at or for the FCC, must return and/or sever all computer access rights. To facilitate this process, Bureau/Office Assistants for Management must submit an email to the "sign out" group announcing the users intended departure. It will be the responsibility of the system administrator to update their respective systems. All files contained in the users directory(ies) will be made available to the user's supervisor once access is terminated. Options available to the supervisor/COTR include transferring files to a different user, transferring the files to diskette, or purging the files from the system, if applicable.

8.5. Emergency System(s) Access Termination. FCC managers, COTRs, or contractor managers who must have computer access authorization revoked or terminated for FCC users in an emergency situation should immediately contact their Bureau/Office Assistants for Management and the Computer Resource Center (CRC). CRC staff will ensure that proper measures are taken to initiate the access termination process. The requestor of an emergency termination action must follow-up with appropriate documentation supporting the request.

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."

It is FCC policy that each FCC user having access to computer resources will attend the FCC Computer Security Awareness Training Program. The program will generally include discussion on the topics of computer security basics, acceptable computer practices, and an overview of computer security policies and procedures. FCC users will be instructed on training dates, times, and location several weeks prior to the training.

9.1. Orientation Training. Each new user of FCC computer systems shall be provided orientation training materials which outline responsibilities on safe computer practices. In addition to the training materials provided, a user can view training videos, which will discuss common sense precautions when operating computer systems, and the user's security responsibilities.

9.2. Annual Training. As with Orientation Training, the objective of the annual training program is to enhance users' knowledge of good security practices while operating FCC computer systems. Training topics will include computer security policy, security planning and management, and general user practices which will maintain an acceptable overall security posture of information and associated systems. The format for different audiences will vary, but the message will be the same.

9.3. Security Briefings. As necessary, security briefings serve to inform specific groups of situations or up-coming events which require computer security related attention (i.e., specific Bureau/Office program needs, etc.).

10. REMOTE FCC NETWORK ACCESS

Appropriate access controls must be in place to support dial-in access to FCC computer systems. Remote interfaces to FCC computer systems will provide similar security to that available when connecting to the system locally. The following guidelines are used by FCC users and ITC System Administrators to facilitate secure dial-in/out communication with FCC computer systems:

- Dial-in ports are protected from unauthorized access.

- Controls are established to ensure that remote users are authenticated before connection to the network is authorized. Further, remote system(s) access using Guest accounts *must* be prohibited. Users must have a unique userID that meets the requirements of section 7.1 of this Directive.

- Users are granted access to only the information for which they are authorized and have a need to access.

- Dial-in to FCC computer systems only occurs through entry points approved by ITC.

- Updates and changes in system communication hardware and software are tested thoroughly to prevent unintentional access exposures.

- Reasonable care is taken to protect communication equipment and telecommunications cables from unauthorized access. Any installation or adjustment of communication equipment is coordinated with the ITC, NDG.

- Users are required to attend training, which includes proper security precautions, before receiving a remote access account.

11. INTERNET ACCESS

Internet access is provided to every FCC user as a resource to directly facilitate work. In addition, accessing the Internet will broaden FCC users understanding of the general structure and availability of resources on the worldwide system of computer networks and how these resources might be applied at the FCC. For these reasons, FCC users are encouraged to explore the wide variety of sites on the Internet. While it is the intention of the FCC to provide access to and encourage exploration of this state-of-the-art computer technology, it is also the Commission's responsibility to manage access to these systems.

11.1. Work Related. Internet access provided by the FCC is intended primarily for work related purposes. To the extent possible, users should become informed of an Internet site's primary information content prior to actually connecting to it. In some cases the site name will be highly revealing. It is the user's responsibility to exercise good judgment when accessing Internet sites and avoid sites that might cause embarrassment to the FCC. For example, Internet sites containing sexually explicit, oriented or related material should not knowingly be accessed using FCC computer resources.

11.2. Limited Personal Use. In addition to accessing web sites in order to learn about their possible applicability to the FCC, users also may make limited personal use of the Internet during non-work time. Such use must not interfere with official duties, must involve minimal impact on the government, and must be consistent with the Standards of Ethical Conduct contained in 5 CFR Part 2635 and Part 19 of the Commission's rules. See below for examples of impermissible uses.

In the past, the Commission has permitted access to the Internet whenever it could be justified as serving a work-related purpose. Consistent with recent guidance applicable to federal agencies, the Commission has determined that it is appropriate to establish a new policy under which employees may make limited personal use of the Internet on non-work time. Non-work time consists of time when users are not otherwise expected to be addressing official business, including before or after work, during lunch and breaks during the day.

11.3. Telecommuters. The policy of allowing limited personal use of the Internet on non-work time applies to all FCC users, including telecommuters. Consistent with the rule that employees may make limited, occasional personal use of this service, the FCC's Internet connection should not be used by telecommuters as a substitute for their own Internet service provider.

11.4. System Monitoring. Each FCC user is identified as a member of the FCC staff and as a member of the Federal government (i.e., John Doe FCC user ID = "jdoe@fcc.gov") when accessing the Internet. Most Internet site managers monitor or audit usage of their site and can provide lists of users to various entities. Further, all Internet connectivity via FCC computer systems is logged and recorded, is an official record, and may be monitored. Inappropriate or illegal activity discovered during routine audits will be forwarded to authorities for appropriate action.

11.5. Impermissible Personal Uses

Inappropriate personal use of computer resources includes:

- Any personal use that could cause congestion, delay, or disruption of service to any government system or equipment. For example, continuous data streams (e.g. video files) or other large file attachments can degrade the performance of the overall functionality of the FCC network and would thus be an inappropriate use.

- Using the FCC systems to launch illegal computer-based attacks or to gain unauthorized access to other systems.

- The creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings regardless of the subject matter.

- Using the FCC system for activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include, but is not limited to: hate speech, or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.

- The creation, download, viewing, storage, copying or transmission of sexually explicit or sexually oriented materials.

- The creation, download, viewing, storage, copying or transmission of materials related to illegal gambling, illegal weapons, terrorist activities, and any other illegal activities.

- Use for commercial purposes or in support of "for-profit" activities or in support of other outside employment or business activity (e.g. consulting for pay, sales or administration of business transactions, sale of goods or services).

- Engaging in any outside fund-raising activity, endorsing any product or service, as provided in 5 CFR 2635 of the Standards of Ethical Conduct.

- Participating in any lobbying activity except as provided by law, or engaging in any prohibited partisan political activity prohibited by law.

- Use for posting agency information to external newsgroups, bulletin boards or other public forums without authority. This includes any use that could create the perception that the communication was made in one's official capacity as a federal employee, unless appropriate Agency approval has been obtained, or use is at odds with the agency's mission or positions.

- The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information including computer software and data, that includes privacy information, copyrighted, trade marked or material with other intellectual property rights (beyond fair use), proprietary data, or export controlled software or data.

12. ELECTRONIC MAIL

The FCC Electronic Mail (email) facility offers FCC users with an efficient way to communicate with others inside, and outside (via Internet) the FCC using Commission computer systems. FCC email is provided for use to accomplish day-to-day business activities.

12.1. Distribution Protocol. Whenever possible, FCC users should limit the distribution of email to the smallest group possible in order to eliminate unnecessary network congestion. If an inappropriate email is brought to the attention of the Computer Security Officer, the "sender" will be directed to retract the message by either the email Postmaster or the Computer Security Officer. The Postmaster will retract inappropriate or unauthorized email if the "sender" is not available.

> **Important Note**: An email message sent to the "Everyone", or similar group, reaches approximately 2,500 FCC employees and contractors throughout the United States. If the message is inappropriate or not authorized for distribution on the FCC network, there is a significant burden on the FCC.

12.2. FCC Email outside the FCC. Authorized FCC email users *are not* permitted to forward FCC email or attachments to personal accounts managed by public email or

Internet access service providers where the information might be compromised. Further, FCC users *are not* authorized to use the email system to send sensitive Commission information via the Internet where information might be intercepted.

12.3. Personal Use. FCC employees may make incidental personal use of email. Any incidental email usage may not interfere with official duties, must have a minimal effect on the government and must be consistent with the Standards of Ethical Conduct.

12.4. Appropriate Use of Electronic Mail. Appropriate use of the FCC email system includes generating and sending emails regarding:

- FCC mission and program related activities.
- EEO, FCCRA, Union Activities and Leave Donation Requests.
- Savings Bond, Combined Federal Campaign and Bloodmobile Drives.
- Other FCC business related and endorsed activities.
- Subject to the limitations contained in this email policy statement, brief occasional personal messages.

12.5. Inappropriate Use of Electronic Mail. The FCC email facility may not be used to direct personal messages to the Everyone Group or other large groups of users. For example, FCC GroupWise email system shall not be used to send or forward messages which may contain Birth and Retirement notices, For Sale or rent notices, Death notices of non-FCC staff, or the like, but rather should be posted on the FCC Bulletin Board System (BBS).

13. DESKTOP SECURITY

The FCC has an approved desktop configuration for workstations that is approved by the Computer Security Officer.

- It is the user's responsibility to control access to data and applications residing on assigned workstations.
- Any security controls in place on the desktop (e.g. antivirus software, screen saver passwords) must remain in place unless authorized by the Computer Security Officer.
- Access to the workstation must be controlled using FCC approved password controls. No modifications may be made to the FCC approved password controls unless authorized by the Computer Security Officer.

14. SOFTWARE MANAGEMENT

Software used and stored on FCC computers must be properly licensed. Non-licensed software is not authorized for use on FCC computers. In addition, software that may have been downloaded or purchased must be pre-authorized for installation on local computer

drive(s). In addition, users are not authorized to place software, which has been licensed for individual use, on any shared drive.

14.1. Installing Non-FCC Standard Software on FCC Computers. At times, FCC users may be required to use computer software programs, which are not readily available at the Commission. Computer resources, including system disk space, are limited agency assets. In order to maximize the use of our computer resources, the group(s) managing the system(s) must be aware of what is loaded on their respective system(s). FCC managers also have the responsibility to ensure that software loaded on Commission computer systems is properly licensed. To support this effort, users must obtain authorization prior to installing software on their local drives by completing the FCC Computer System Personally-Owned Software Certification, Form A-202 (attached) and submitting the form to the Computer Resource Center for processing. Conditions which will be considered prior to approving a request, include:

- Is the software to be installed intended to support official FCC business?
- Is the software only to be loaded on the user's local computer drive(s)?
- Has the software been scanned to ensure there are no computer viruses resident on the diskette(s)?
- Will the software encumber related FCC computer resources?

14.2. Single License Software. FCC users should ensure that single license software programs are not loaded on shared system drives (i.e., J:\, M:\, etc.) or shared with others, but rather loaded only on local computer drives, once approved. Software inappropriately loaded or loaded without proper approval on system shared drives may be purged from the system after notice has been given to the user(s).

14.3. 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 Computer Resource Center for assistance.

14.4. Upgrading Software. As necessary, software will be upgraded to a newer or up-to-date version, provided funding is available. When previous versions of software are no longer installed on FCC computer systems or individual PCs, appropriate actions should be taken to ensure destruction of the old version, ensuring the software is no longer useable.

14.5. Games. Users of FCC computer resources are *not* authorized to load games software on FCC provided computer systems.

15. COMPUTER VIRUS PREVENTION AND MANAGEMENT

A virus is a piece of computer programming code usually disguised as something else that causes some unexpected and, for the victim, often an undesirable outcome. Some viruses are programmed so that they automatically spread to other computer users. Viruses can be transmitted as attachments to an email, downloaded from Internet sites, or copied from diskettes or CD. The source of the email, downloaded file, or other source of the infected file is often unaware of the virus. Some viruses wreak their effect as soon as their code is executed; other viruses lie dormant until circumstances cause their code to be executed by the computer. Some viruses are playful in intent and effect (e.g., "Happy Birthday!"). Others can be quite harmful, erasing data causing email systems to overload, and/or causing severe network outages.

The best protection against a virus is to know the origin of each program or file loaded into the computer or opened from the email program. In addition all FCC computers are supplied with antivirus software that can screen email attachments and also check all of a user's files periodically and remove any viruses that are found. From time to time, users may receive an email message warning of a new virus. Unless the warning is from the FCC Computer Security Officer, or a recognized source, chances are good that the warning is a virus hoax. It is suggested that FCC users forward any warning received from non-FCC sources to the FCC Computer Security Officer for validation.

FCC computer system users can minimize exposure to viruses by following these safe-computing practices (additional guidance is available by contacting either the CRC or the Computer Security Officer):

- Place write-protection on original software diskettes.
- Do not use unauthorized software.
- Never download programs from the Internet to the office PCs without scanning the file to be downloaded.
- Do not use shareware and demonstration software from unauthorized sources or unfamiliar vendors.
- Use an up-to-date, FCC approved antivirus program. ITC, Operations Group 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 FCC Users, or outside sources. If a virus is detected, the user should notify the CRC immediately.
- FCC users should extend the layer of virus protection to home computers by installing antivirus software on home computers. If there is not an up-to-date antivirus program on a home computer, the FCC has antivirus CDs available for home use. Apply similar antivirus precautions on the home computer as described, herein.

- Be suspicious of email attachments. Always scan executable email attachments before opening. Many infected files transmit themselves through email programs. Just because the person sending the file is known does not mean it is virus free.

- Check to ensure that Microsoft Office Applications have macro protection enabled. Once this is done, if a file is opened with a macro virus it will prompt to Enable or Disable macros. Always choose *Disable Macros* or *Do Not Open* if a Macro Dialog Protection Warning is received for a document not expected to contain macros.

- Reboot PCs at least once a day to ensure that the latest antivirus definitions are received.

16. 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:

16.1. 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, system-provided mandatory *Screen Saver* and associated password are imposed for each user of FCC PCs. 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.

16.2. Preventing Hardware Theft. Information and computer equipment must be protected against heft. 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 or has a business or economic impact. It is recommended that Bureaus/Offices select and implement security controls that employ any or all of the following measures:

- *Do not* store critical or sensitive data, files, or programs on any PC's local drive. Rather, store such information on the local file server (e.g. N:\ Drive). As deemed necessary by each user, periodically backup any files stored on the local computer's drive to diskette and store in a safe and secure location.

- 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.

- Business sensitive correspondence, other printed information and magnetic media should be stored in locked containers, desks or file cabinets;

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

16.3. Portable Computer Resources. Portable computer resources (e.g., Laptop, Notebook, Personal Digital Assistant, etc.) provide convenience and productivity gains. However, with portable computer resources there are increased risks of theft and loss of information.

Hardware and software techniques should be employed to keep FCC information protected from unauthorized individuals in the event the portable equipment is lost or stolen. Options include, but are not limited to, lock-down devices and PC-boot passwords.

- FCC users should be particularly security conscious when traveling with portable computer resources.

- FCC users should not check FCC assigned laptop computer as baggage when traveling with commercial carriers, rather maintain possession of the laptop at all times.

Security and inventory play a key role in the management of portable computer resources. All portable resources should be kept secured in a locked storage area while stocked. Staff responsible for the management of inventory should maintain records to include, as a minimum:

- a master inventory list of all portable equipment assigned
- user's name checking out the resource
- equipment brand name
- equipment serial, bar code, and FCC numbers
- fax modem card number
- a copy of the FCC Property Pass slip

16.4. Removable Information Media. Removable media (e.g., tapes, CD-ROM, CD-R, Zip disks, floppy diskettes, etc.) allow for the storage of large concentrations of

sensitive data vital to the FCC mission. Depending on the potential exposure of information residing on removable media, managers should establish any or all of the following controls:

- Ensure that FCC users understand the significance of sensitive information contained on removable media. Additionally, advise FCC users of their responsibility to protect information on removable media as protection of this information would be required in other formats.

- Discard hard-copy information in a secure manner that prohibits the information from being retrieved and made use of by unauthorized persons.

- Develop procedures to ensure that sensitive information is not stored on diskettes unless the diskettes are properly labeled and stored in a lockable unit in an access-controlled environment.

- Encourage the use of document password controls available with FCC provided desktop applications.

16.5. Relocating Computer Hardware. PCs and related hardware are often moved from one location to another. It is important that secure methods are employed to safeguard this equipment and the information it may contain during relocation. FCC users should submit a Move Questionnaire to the building management center, requesting the relocation of computer hardware, which is then forwarded to the Operations Group (OG). OG completes the move and maintains the validity of the equipment inventory. Each Bureau/Office may consider an internal process to ensure clearance through the Assistant for Management before releasing the move request to OG.

16.6. 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 are installed to mitigate the possibility of power spikes for incoming power supplies. In addition, surge protectors should be used on all FCC issued computers. Battery backup via an uninterruptible power supply (UPS) must be installed to provide system server(s) and peripherals support in the event of a power failure.

16.7. Telecommuting. All FCC owned computers and other equipment relocated to an employee's home for telecommuting purposes are covered by this directive. Hardware and software techniques should be employed to keep FCC information protected from unauthorized individuals. Also, passwords should be safeguarded to prevent access by unauthorized individuals to the FCC network.

17. COMPUTER SYSTEM BUSINESS RECOVERY

17.1. PC Data Backups. Users are instructed not to store sensitive or mission critical data on their PCs hard-drive. Users are instructed to store all sensitive and mission-critical data on the network server. However, any data that is stored on the PC's hard-drive should be protected from inadvertent loss. As a precautionary measure, users are encouraged to backup data to diskette at an interval commensurate with how often data changes are made, and secure the diskette(s) in a safe location.

17.2. Application and Data Backups. To be usable, copies of electronic media must be made accurately, regularly, and consistently. ITC Operations Group ensures that adequate network backups 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. Bureau/Office application managers shall ensure that adequate backups are made of bureau/office applications/databases, and data within their control.

In all cases, System Managers will use the 'son, father, and grandfather' system, the following should be considered as minimum standards in the backup process:

- Incremental (or differential) backups (data files that have been modified) should be taken daily.
- System backups (all data files) should be taken weekly.
- Application configuration backups should be taken monthly.

The means by which electronic backups are stored is as important as the backup process. The most recent backups, incremental and system, should be stored on-site for immediate access, as needed. These backup tapes must be stored in a safe location capable of protecting electronic media from environmental (e.g., fire, water, smoke, etc) concerns. After the new version of the backups are completed, the previous version must be stored off-site (ie., a different location than that of the system and current backups.) As the series of backups are made, the oldest version stored off-site should be returned to the operations site for reuse.

The current retention policy for system and data backups is to hold twelve weeks of data in the backup program (one week in the on-site safe, ten weeks at the off-site storage facility, with the final week processed back to the FCC from the off-site storage facility). The off-site location should provide similar protection against environmental threats and physical access, as that of the Computer Room. A similar backup process should be considered for independent computer systems.

17.3. Computer Incident Response Team. The FCC's Computer Incident Response Team (CIRT) has been charged to act as the Commission's focal point for

mitigating the impact of computer related incidents. The team is comprised of technical experts in the fields of PCs, computer networks, telecommunications, application(s) management, and security. As required, the team acts to prevent or minimize the impact of a threat against computer operations at the FCC (e.g., isolating a computer virus infection and eradicating its infection without the destruction of data, implementing the teams mitigation plan to prevent intruders from accessing FCC computer systems, taking preliminary steps to minimize the need for the agency's COOP, etc).

17.4. Continuity of Operations Plan. Although some risks can be minimized, they cannot be eliminated. Undesirable events occur regardless of the effectiveness of a security/control program. The Continuity of Operations Plan (COOP) provides a controlled response that minimizes damage and restores operations as quickly as possible. The COOP consists of a document that provides a course of action to be followed before, during, and after the occurrence of an undesirable event that disrupts or interrupts network operations. ITC is responsible to develop and periodically test the FCC COOP. Bureau/Office representatives involved in the implementation of the COOP will be briefed in advance and will receive a copy of the plan. The COOP will be updated annually to reflect changes in the FCC's architecture and mission priorities.

18. PERSONNEL SECURITY

As mandated by Executive Order 12968, Executive Order 10450 and OPM, 5CFR731, the FCC must conduct personnel security and suitability investigations. Each FCC User will be classified as a High, Moderate or Low Risk according to level of access to the respective systems. Background investigations will be conducted to ensure compliance with Federal Mandates.

19. 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 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 ITC CIO's responsibilities for compliance with computer security requirements.

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

- Acknowledge responsibility of resources and identify those applications 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.

20. SENSITIVE/MISSION CRITICAL DATA

As mandated in the Computer Security Act of 1987, the FCC must determine the classification of sensitive data in its possession. Each FCC Bureau/Office owning or acting as custodian of computer based application is responsible for determining the sensitivity of those documents. The Bureau/Office representative making such decisions must consult PERM for concurrence.

Based on the National Institute of Standards and Technology (NIST) guidelines, the following criteria to determine the sensitivity and/or related mission critical nature of applications and data processed at the FCC applies:

- Information protected under the Privacy Act of 1974 and the Freedom of Information Act.
- Data and information, which is critical to an agency's ability to perform its mission.
- Financial Management Data on systems that process electronic funds transfers, control inventory, issue checks, control accounts receivable and payable, etc.
- Each Bureau/Office shall ensure that all computer-processed data created be identified. ITC must be notified, via memorandum, of all sensitive and mission critical data generated or processed by a Bureau/Office computer based application. Ad-hoc output reports shall be safeguarded in a manner commensurate with the standards established in this and the following sections.

21. SAFEGUARDING SENSITIVE/MISSION CRITICAL DATA

Each FCC Bureau/Office shall be responsible for ensuring that all forms of media (e.g., paper, diskette, CD-ROMs, cartridge, etc.) containing sensitive data originated or processed by the Bureau/Office is handled and disposed of in a manner commensurate with the criteria established in this and other FCC directives (20.1 Storing Sensitive Data). FCC users should ensure that sensitive data is not stored on shared drives (i.e., J:\ drive) where many users may have uncontrolled access to the data. In addition, users should *not* store sensitive data on their local drive (i.e., C:\). Bureaus/Offices and users requiring a secure method for sharing sensitive information should consider the use of the Novell Netware Filer utility. If properly configured, Filer safely allows multiple users to share documents in a common area (i.e., J: drive). By establishing a sub-directory using Filer, access can be controlled, allowing the custodian to define who has access to the sub-directory. The CRC can assist in setting up such sub-directories.

21.1. Sharing Sensitive and Other Data with Others Outside the FCC. It is the policy of the FCC that Sensitive Information (Non-Public—For Internal Use Only, Non-Public—Highly Sensitive/Restricted, financial and other types of data) only releasable by authorized Bureaus/Offices within the FCC. Further, users should

take precautions to protect the release of magnetic media containing sensitive information and should contact their supervisor for guidance, as needed.

22. 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. The following procedures, or other processes supporting similar security procedures, should be considered within each Bureau/Office for the disposal of such reports:

- Sensitive documents should not be hoarded, but destroyed as soon as they are no longer required.
- Electronic media (diskettes, magnetic tapes, CD-ROMs, etc.) should be destroyed, or over-written.
- Material that is no longer needed and may lawfully be destroyed must be disposed of in a locked document disposal bin (in the Portals building) or other comparable method (in non-headquarters locations.)

23. IDENTIFYING SENSITIVE/MISSION CRITICAL APPLICATIONS

The term sensitive application, as defined by OMB Circular A-130, means "an application of information technology that requires protection because it processes sensitive data, or because of the risk or magnitude of loss or harm that could result from improper operation or deliberate manipulation of the application." As such, Bureaus/Offices are required to determine and notify ITC of which, if any, applications/databases controlled or utilized within that Bureau/Office are considered sensitive or support a function considered critical to the successful operation of the FCC. The information provided will become a crucial component of the Commission's COOP.

24. SENSITIVE/MISSION CRITICAL AND MAJOR APPLICATION – CERTIFICATION AND ACCREDITATION

At various times, computer applications will be created and utilized at the FCC, which process sensitive data. Prior to implementation, these applications shall undergo testing to verify that the required administrative and technical safeguards are operationally adequate and the results of the design review and system tests are fully documented and maintained. ITC in concert with the Bureau/Office managing the design of a new application/database which is intended to process sensitive data should select and assign qualified personnel to test the security of the application. Should an application require significant expansion or revision, the series of tests should re-occur. The Computer Security Officer can provide technical oversight support during all phases, as requested by the Bureau.

The personnel assigned the responsibility for system testing shall:

- Establish objectives and specifications required for security of the application.

- Define the security requirements to be included in the design of the application.

- Ensure that all security requirements included in the design phase are incorporated during the programming phases of the application.

- Consider results of the most recent network risk analysis during the application development planning phase to ensure that adequate safeguards are considered.

- Test the security of the application as it interacts with existing operational security controls on the system, and evaluate unexpected or fraudulent inputs to determine the performance of the application during unusual circumstances.

- Ensure the conduct of risk analysis for the application, as required by applicable Federal regulations.

25. SENSITIVE/MISSION CRITICAL SYSTEM CERTIFICATION

Sensitive system certification is intended to provide assurance that sensitive applications meet security related Federal regulations, as required by OMB Circular A-130, Appendix III. The certification process agreed to by the Bureau/Office Manager and the Computer Security Officer, will ensure security safeguards installed during the certification will remain in effect. Each Bureau/Office Manager and the Computer Security Officer should coordinate to complete the certification process for existing/new applications not yet certified. Re-certification of sensitive applications will occur whenever an application is modified significantly or every three years.

26. EXTERNAL COMPUTER RESOURCE SERVICES

FCC computer security directives and policies have no exclusionary provisions, but are applicable to computer systems and information/applications containing FCC information for which the FCC is the legal custodian. The boundaries of responsibility apply whether the processing services are performed at an FCC facility, by another Government agency, or by a non-government agency (i.e., contractor.)

26.1. Sensitive FCC Data Processed by another Government Agency. All Government agencies are required to adhere to the information security policies in OMB Circular A-130 unless more stringent policies or regulations apply at the agency where the information is being processed. Regardless of the approach, all Government agencies must adhere to the policy that sensitive applications will only be processed on computer systems having appropriate security protection, after sensitive applications have been certified to handle sensitive data by the Bureau/Office Manager and the Computer Security Officer.

26.1.1. It is the responsibility of the COTR, with the assistance of ITC, PERM, to determine the level of sensitivity of the data to be processed by the external organization. The computer security requirements will be made

known to the external organization during contract negotiations and prior to any contract initiation.

26.1.2. Sensitive information will be processed only on systems having appropriate security protection and which have been certified to handle such information. If the computer system is not under the control of the FCC, the certification document will be requested from the custodian/owner of the system.

26.1.3. Copies of the certification documents, provided by the outside organization, and any relevant correspondence should be maintained by the COTR.

26.1.4. Re-certification of sensitive systems or applications must be accomplished by the external organization, within the time frames set-forth in applicable Federal regulations. The data processing agreement with the organization should state that the re-certification will be accomplished as required, and that a copy of the certificate will be provided to the Computer Security Officer.

26.2. Sensitive FCC Data Processed by a Non-Government Agency. More and more Government work is being performed by non-Government agencies (i.e., contractors.) When these organizations are under contract with the FCC, the contract must specify adherence to the FCC Computer Security Program Directives. In addition:

26.2.1. Before entering into an agreement to process or handle sensitive information at a contractor facility, a security assessment of the facility should be conducted, or should have been completed within the previous three years, and the results of the analysis will be made available to the Contracting Officer for review. The Contracting Officer should consult the Computer Security Officer for technical assistance, as required.

26.2.2. The contract should specify that FCC reserves the right to perform unannounced on-site inspections of the site where FCC information is being processed. The inspections are used as a tool to ensure adherence to FCC's computer security directive and policies, and other applicable Federal regulations and mandates.

26.2.3. The COTR will monitor contractor compliance with FCC's Computer Security Program Directive and policies, therein.

27. COMPUTER SYSTEM(S) SECURITY AUDITS

At periodic intervals, it is necessary that audits be performed on FCC computer systems and applications. The primary focus for security audits of computer systems is to ensure that unauthorized or illegal activities are detected and remedied as quickly as possible. Secondary benefits to system audits support the organization's administration and management function.

For instance, routine audits of computer systems will ensure that only authorized users have access to the system/information; appropriate levels of access have been authorized and are maintained; and that previously authorized users of a system no longer requiring access are purged.

28. INCIDENT AND VIOLATION REPORTING

When a breach of computer systems security occurs (i.e., unauthorized disclosure, alteration, destruction, loss or compromise of sensitive data, resources and unauthorized access, or misuse of computer resources), incident and violation reporting serves as a means of resolution. It is imperative that any security breach be isolated and contained allowing appropriate personnel to respond to the situation. FCC users are responsible, as described in *Responsibilities* section of this directive, for promptly reporting computer system security related incidents to the Computer Security Officer.

The Computer Security Officer will coordinate with respective ITC managers, the Inspector General, and the Bureau/Office to inquire into reported information and computer security violations and collect, develop, and retain sufficient information to bring the reported computer security violation to closure.

Andrew S. Fishel
Managing Director

- FCC Computer System Security Acknowledgement, Form A-201
- FCC Computer System Personally-Owned Software Certification, Form A-202
- FCC Computer System Separation Clearance, Form A-203
- Definitions
- References

Stocked By:
Performance Evaluation and Records Management

DEFINITIONS

a. Access - 1. The ability to enter a secured area. 2. A specific type of information between a subject and an object that results in the flow of information from one to the other.

b. Access Control - An entire set of procedures performed by hardware, software, and administrators to monitor access, identify users requesting access, record access attempts, and grant or deny access based on pre-established rules.

c. Adequate security - security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.

d. Alphanumeric - A contraction of *alphabetic* and *numeric*, that indicates a combination of *any* letters, numbers, and special characters.

e. Application - means the use of information resources (information and information technology) to satisfy a specific set of user requirements.

f. Availability - That aspect of security that deals with the timely delivery of information and services to the user.

g. Backup - Applies to data, equipment or procedures that are available for use in the event of failure or loss of normally used data, equipment or procedures. The provision of adequate backup capability and facilities is important to the design of data processing systems in the event of a system failure that may potentially bring the operations of the business to a virtual standstill.

h. Computer Log-in - A simple procedure occurring at the beginning of a session at a workstation in which the host asks the user for identification. At the FCC, login refers to two separate authorization codes: userID, and password.

   1. UserID is the authorization code used to verify that FCC users are entitled access to FCC computer resources, and to identify the specific resource(s) used; and

   2. Password is a unique secret word selected by each user that is associated with a particular user ID. The Passwords primary function is to protect the userID from unauthorized use. A non-display mode is used when the password is entered to prevent disclosure to others.

i. Computer Security - Technological and managerial procedures applied to computer systems to ensure the availability, integrity, and confidentiality of information managed by the computer system.

j. Data Integrity - A measure of data quality. Integrity is high when undetected errors in a database are few. Complete data integrity is the assurance that is input to the computer today will be there tomorrow, unchanged in any way.

k. Bureau/Office Manager - Any FCC Bureau/Office representative who acts as the application/database or system focal point for management.

l. General Support Systems - Are those interconnected set of information resources under the same direct management control which share common functionality. A system can be, for example, a local area network or an agency-wide backbone.

m. Hardcopy - Medium of data, either input or output, in paper form such as printouts, reports, screen prints, memoranda, checks, etc. generated as a result of the use of FCC computer system resources.

n. Major Application - An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.

o. Mission Critical Data - Is any electronic data which supports the collection, transfer, or disbursement of funds, or Commission activities mandated by statue or treaty, the interruption of which would cause significant economic or social harm to licensees or the public.

p. Removable Media - An information storage medium that can be removed from an information creation device such as a computer. Examples are diskettes, tapes, cartridges, optical disks, and external disk drives.

q. Sensitive Information - Is that which requires various degrees of protection due to the risk and magnitude of loss or harm, which could result from accidental or deliberate disclosure, alteration, or destruction. This data includes records protected from disclosure by the Privacy Act, as well as information that may be withheld under the Freedom of Information Act, Non-Public—Highly Sensitive/Restricted and/or Non-Public—For Internal Use Only. Computer "hard copy" is considered, for purposes of this directive, a computerized record, and may contain "sensitive" data.

REFERENCES

a. Public Law 99-474, Subject: "Computer Fraud and Abuse Act of 1986." The act provides for unlimited fines and imprisonment of up to 20 years if a person "intentionally accesses a computer without authorization or exceeds authorized access and, by means of such conduct, obtains information that has been determined...to require protection against unauthorized disclosure...." It is also an offense if a person intentionally accesses "a Federal interest computer without authorization and, by means of one or more instances of such conduct alters, damages, or destroys information...or prevents authorized use of such computer...or traffics any password or similar information...if such computer is used by or for the Government or the United States."

b. Public Law 100-235, Subject: "Computer Security Act of 1987." The Act provides for a computer standards program within the National Institute of Standards and Technology (NIST), to provide for Government-wide computer security, and to provide for the training in security matters of persons who are involved in the management, operation, and use of Federal computer systems, and for other purposes.

c. OMB Circular No. A-123, Revised, Subject: "Internal Control Systems." Requires heads of government agencies establish and maintain effective systems of internal control within their agencies that, in part, safeguard its assets against waste, loss, unauthorized use, and misappropriation. Among other things, the circular specifies that periodic security reviews be conducted to determine if resources are being misused.

d. OMB Circular No. A-127, Subject: "Financial Management Systems." This Circular prescribes policies and procedures to be followed by executive departments and agencies in developing, operating, evaluating, and reporting on financial management systems.

e. OMB Circular No. A-130 "Management of Federal Information Resources," Appendix III "Security of Federal Automated Information Resources." Requires federal agencies to implement a computer security program and develop physical, administrative, and technical controls to safeguard personal, proprietary, and other sensitive data in automated data systems. OMB Circular A-130 also requires that periodic audits and reviews be conducted to certify or recertify the adequacy of these safeguards. In addition, it makes agency heads responsible for limiting the collection of individually identifiable information and proprietary information to that which is legally authorized and necessary for the proper performance of agency functions, and to develop procedures to periodically review the agency's information resources to ensure conformity.

f. 5 CFR Part 2635.11-12, "Standards of Ethical Conduct for Employees of the Executive Branch." Use of Government Property - Personnel shall protect and conserve Government property, including equipment, supplies and other property entrusted to them. Use of Government Information - Personnel shall not use, or allow use of, official information obtained through performance of duties to further a private interest if such information is not available to the general public.

g. 5 USC 552, Freedom of Information Act (FOIA) of 1974, As Amended. FOIA requires agencies to make available, on its own initiative, certain types of records and disclose any other record to a requestor unless a specific exemption under FOIA, of which there are nine, applies.

h. 5 USC 552a, Privacy Act of 1974, As Amended. The basic provisions of the act are to protect the privacy of individuals. An agency is prohibited from disclosing personal information contained in a system of records to anyone or another agency unless the individual (about whom the information pertains) makes a written request or gives prior written consent for third party disclosure (to another individual or agency).

i. 40 United States Code 1452, Clinger-Cohen Act of 1996. This Act links security to agency capital planning and budget processes, establishes agency Chief Information Officers, and re-codifies the Computer Security Act of 1987.

j. NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems. This publication details the specific controls that should be documented in a security plan.

k. Paperwork Reduction Act of 1995. This Act linked security to agency capital planning and budget processes, established agency Chief Information Officers, and re-codified the Computer Security Act of 1987.

l. Federal Information Processing Standards (FIPS) Pub. 102, Guideline for Computer Security Certification and Accreditation. This guideline describes how to establish and how to carry out a certification and accreditation program for computer security.

m. GAO/AIMD-12.19.6, Federal Information System Controls Audit Manual (FISCAM). The FISCAM methodology provides guidance to auditors in evaluating internal controls over the confidentiality, integrity, and availability of data maintained in computer-based information systems.

n. P.L.106-398, The FY 2001 Defense Authorization Act including Title X, subtitle G, "Government Information Security Reform Act." The Act primarily addresses the program management and evaluation aspects of security. It provides a comprehensive framework for establishing and ensuring the effectiveness of controls over information resources that support federal operations.

o. National Information Assurance Certification and Accreditation Process (NIACAP). This process (NSTISSI 1000) establishes a standard national process, set of activities, general tasks, and a management structure to certify and accredit systems that will maintain the Information Assurance (IA) and security posture of a system or site.

p. Presidential Decision Directive 63, "Protecting America's Critical Infrastructures." This directive specifies agency responsibilities for protecting the nation's infrastructure; assessing vulnerabilities of public and private sectors; and eliminating vulnerabilities.