FCC Computer Security
Desk Reference

Computer Incident Response Team

Operational Control
Guide No. OC-291

July 2002

Federal Communications Commission
Office of the Managing Director
Information Technology Center
Computer Security Program

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Purpose

The purpose of the FCC's Computer Incident Response Team (CIRT) is to establish roles, responsibilities, and communications procedures for responding to computer security incidents at the FCC. It establishes teams with the technical and procedural means to appropriately handle and report security incidents. This guide is designed to be used in conjunction with *FCC Computer Security Desk Reference Number OC-290, "Computer Incident Response Guide."*

The primary objective in the formation of the FCC CIRT policy is to establish teams within FCC's Information Technology Center (ITC) to offer quick response to computer security incidents in order to mitigate risks before substantial damage occurs. The CIRT also handles incidents that might otherwise interrupt the day-to-day operation of the FCC's Information Technology (IT) systems or require the FCC to invoke its Continuity of Operations Plan (COOP). The benefit of such teams is the capability to *contain* and *repair* damage from incidents, and *prevent* future damage.

A secondary objective of this effort is to define the Computer Security Officer's (CSO) role in coordinating and reporting computer security incident activities. Other beneficial services from the CIRT capability include the sharing of information within the ITC, enhancing communications with customers, and the ITC's ability to enhance its Computer Security Awareness Training programs for FCC employees and staff.

1.2 Background

FCC computer systems are subject to a wide range of mishaps including corrupted data files, to viruses, to natural disasters. Some of these mishaps can be fixed through day-to-day operating procedures. For example, frequently occurring events (e.g., a mistakenly deleted file) can usually be readily repaired (e.g., by restoration from the backup file). More severe mishaps, such as outages caused by natural disasters, will normally be addressed in an ITC COOP. Other damaging events result from deliberate malicious technical activity (e.g., the creation of viruses or system hacking).

Such activity can be initiated from an outsider (non-FCC system user) or an insider (FCC system user.) This policy establishes roles, responsibilities, and communications procedures for handling computer security incidents. Although the threats that hackers and malicious code pose to systems and networks are well known**,** the occurrence of such harmful events remains unpredictable.

This document, along with other FCC security policies and documentation, helps to address the Office of Management and Budget (OMB) Circular No. A-130, Appendix III requirements for the FCC to "Protect government information commensurate with the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of such information."

1.3 Scope

The guidance contained in this document applies to all IT support staff, i.e., system administrators, application owners, the Auctions Operations Group, and ITC personnel. This guidance is applicable to all FCC information and infrastructure computing resources, at all levels of sensitivity, whether owned and operated by the FCC or operated on behalf of the FCC.

1.4 Authority

This document is issued pursuant to the Government Information Security Reform Act (Public Law 106-398, Title X, subtitle G) requirement for agencies to "develop and implement an agency-wide information security program" that includes "procedures for detecting, reporting, and responding to security incidents…."

This document also helps to satisfy FCC Directive FCCINST 1479.2, section 6.3.10 that requires the FCC's CSO to "manage the ITC's Computer Incident Response Team (CIRT)."

1.5 Roles and Responsibilities

1.5.1 FCC Personnel

Users, administrators, application owners, and managers of FCC systems are responsible for reporting suspected computer security incidents to the FCC's Computer Resource Center (CRC).

1.5.2 FCC Computer Security Officer

The CSO performs the following actions to ensure coordination and proper functioning of the FCC's CIRT.

- Receives notification from the FCC's CRC or from outside sources.
- Activates the CIRT.
- Briefs the Chief Information Officer (CIO) and Deputy CIO as necessary throughout the incident.
- Informs the FCC's Office of the Inspector General (OIG) of the incident.
- Notifies the appropriate Customer Service Representative (CSR) of the affected bureau/office.
- Contacts outside law enforcement and government agencies as necessary.
- Maintains the CIRT policy, procedures, and roster.
- Conducts periodic updates and process reviews with the various CIRTs.

1.5.3 FCC Computer Resource Center

The FCC's CRC (i.e. help desk) performs the following actions related to computer security incident response.

- Receives reports of computer security incidents from FCC customers during working hours through the internal Computer Help Desk phone number.
- Receives reports of computer security incidents from FCC customers during non-working hours by means of an emergency cell phone number, which is listed on the CIRT roster.
- Identifies threat to FCC Systems (malicious internal user or external intruder).
- Notifies the CSO.
- Tracks the incident by opening a trouble ticket.
- Follows up with the CSO to verify effective resolution of the incident before closing the ticket.

1.5.4 FCC CIRT Members

Each member of the CIRT is responsible for the following actions related to FCC's CIRT program.

- Responds to activities that might interrupt the IT services of the area for which the team is responsible during working and non-working hours.
- Investigates incidents, assists with recovery efforts, documents incidents, and provides regular reports to the CSO.
- Maintains awareness of and follows procedures for effective response to computer security incidents.
- Stays current on functional and security operations for the technologies within their area of responsibility.
- Follows the direction of the CSO during incident response activities.
- Maintains confidentiality of information related to computer security incidents.
- Participates in periodic updates and process reviews conducted by the CSO.

2 FCC CIRT TEAMS

This policy establishes four groups within the FCC CIRT to handle incidents related to systems that support critical FCC operations.

2.1 UNIX/Linux CIRT

Responds to all activities that might interrupt the services of the UNIX/Linux operating systems owned and managed by the FCC. This includes those systems both inside and outside the FCC firewall (e.g., FCC Web Servers, TIS Gauntlet Firewalls, Routers, all regional field office servers.)

2.2 Novell CIRT

Responds to all activities that might interrupt the services of the Novell operating systems owned and managed by the FCC. This includes all file servers located in the Washington, DC, Columbia, MD, Gettysburg, PA, and all FCC regional and field offices.

2.3 AIS CIRT

Responds to all activities that might interrupt the services of any FCC proprietary applications and databases owned and managed by the FCC and its Bureaus and Offices.

2.4 Auctions CIRT

Responds to all activities that might interrupt the services of any FCC, WTB Auctions activity on the Auctions sub-net. This includes all file servers, UNIX-based operating systems, routers and dial-in ports.

2.5 Microsoft NT/Windows CIRT

Responds to all activities that might interrupt the services of NT- and Windows-based servers and PCs owned and managed by the FCC and its Bureaus and Offices.

3 FCC CIRT ROSTER

The CSO has compiled a roster of names and contact numbers for CIRT members. This roster contains confidential contact information and is authorized for limited distribution to CIRT members and the CRC. Please contact the CSO if you require a copy of the CIRT roster. In addition, the CRC, the IT Operations Group, and the Auctions Group will maintain a copy of the CIRT roster.

4 FCC CIRT PROCEDURES

4.1 Identifying the Customer

ITC customers include computer users of FCC networks (all FCC employees and contractors), program managers and application owners, and others who use or share our computing resources. As you might expect, the customer is not always the entire Commission. For example, an FCC CIRT situation might affect only the Collection System and its users, with no outward affect on others within the Commission. Conversely, the impact of a computer virus might affect the entire FCC computer network population. In a third scenario, the event only may affect FCC field offices. Scenarios also may arise where FCC system users are not affected, but persons who access information from the FCC Web Sites may be.

In each situation, the CSO must identify and inform the customer of the situation. In doing so, the CSO will have a reasonable assessment of the impact on the system and its users and the expectation for resolution. It is through the reporting scheme of such events that the CSO can help to ensure that accurate information is relayed to the customer and those affected by a system outage.

4.2 Computer Resource Center Support and Operations

When an FCC customer reports a potential incident, the CRC makes an initial determination regarding the threat to the FCC's systems. Threat generally results from unauthorized intrusion/attack by outsiders or from unauthorized activities by potentially malicious internal users. The CRC will open a trouble ticket and relay the incident to the CSO, who will initiate the first response to the incident. Once the incident has been resolved, the CRC will consult with the CSO and close out the ticket.

4.3 System and Data Backup

The FCC's Network Operations Group (NOG) provides automated data protection/backup services, maintains the FCC tape library, and manages off-site tape storage for systems managed by the FCC's Information Technology Center (ITC). The NOG can support the CIRT by recovering older versions of data and system files to assist with investigations. The CIRT should work closely with the NOG during efforts to restore systems that may have been damaged or compromised. In some cases, back up and recovery services are provided by the local organization.

The CIRT should contact the CRC to request that the NOG (or other personnel, as appropriate) make electronic data backups available. The NOG will coordinate efforts to recover backups from onsite storage or from the off-site storage facility, as necessary.

4.4 FCC CIRT Communication and Reporting

4.4.1 Reporting Computer Security Incidents

Successful incident handling requires that customers be able to report incidents in a convenient, straightforward fashion. *FCC personnel who identify a potential computer security incident should report the incident directly to the FCC CRC immediately*. The CRC's involvement in the CIRT process provides a central point of communication and tracking of security incidents.

For more information on incident reporting, see *FCC Computer Security Desk Reference Number OC-290, "Computer Incident Response Guide."* This reference guide may be viewed at:

http://intranet.fcc.gov/omd/itc/csg/incident_response_guide/

4.4.2 Rapid Customer Communications Capability

Rapid communication is essential for quickly communicating with the customer as well as with management officials. Whenever feasible, the CSO will issue priority electronic mail messages, containing a Computer Security Alert, to those customers affected by the incident. As necessary, the CSO will utilize other forms of communication including Commission-wide voice mail, and Bureau or group emergency briefings.

4.4.3 Communication with Outside Organizations

Due to increasing computer connectivity, intruder activity on networks can affect many organizations, inside and outside the FCC. The CSO will determine whether activity at the FCC may present a threat to other government organizations and will contact outside authorities as appropriate.

At times, the FCC may require support from investigative agencies, such as federal (e.g., the FBI, Department of Justice), state, and local law enforcement authorities. In addition, the General Services Administration's Federal Computer Incident Response Center (FedCIRC) and the National Infrastructure Protection Center (NIPC) may be consulted when appropriate.

In all instances, the CSO, in consultation with the CIO, will determine when communication with outside organizations is appropriate. The CIRT and other FCC employees must follow the CSO's direction and must not share information regarding an incident outside the FCC without authorization.

4.4.4 Communication with the Office of the Inspector General

Office of Management and Budget (OMB) directives require agencies to include the OIG "as an integral part of the reporting process." As a result, incident reporting to the CIO will include the FCC's Office of the OIG in the reporting process. The CSO will brief the FCC's Inspector General and/or his designee(s) within 48 hours after an incident. The CSO will submit a written report to the OIG within 30 days describing the incident and its resolution.

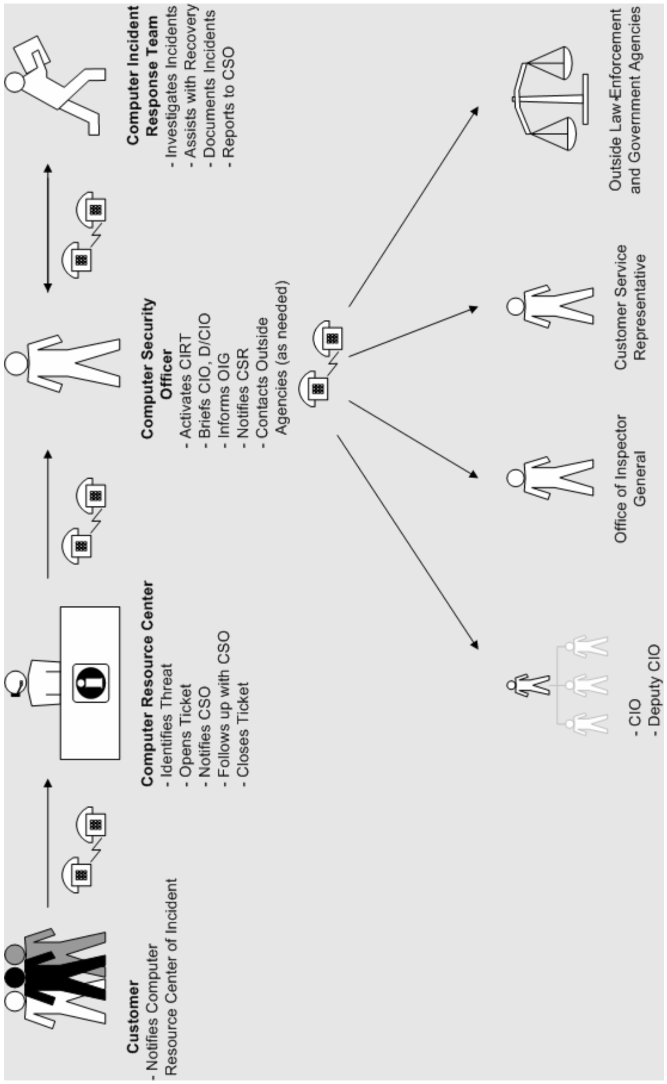
4.4.5 Information Sharing

The CSO routinely conducts assessments of key FCC computer systems. Making such information available to FCC CIRT team members should heighten the awareness of the risk associated with those systems. In addition, by offering informational briefings, cross platform briefings can expand the general understanding of the different operating system platform administrators (e.g., the UNIX team hosts an awareness briefing for other team groups on the current status of the UNIX platform and visa-versa).

4.4.6 Periodic CIRT Meetings

To ensure an open line of communication, the CSO will conduct periodic meetings of CIRT members. These meetings will provide team members with a general understanding of the responsibilities assigned to each CIRT and the types of response scenarios to expect. While the CSO may call emergency meetings on an as needed basis, periodic meetings will be scheduled weeks in advance to ensure attendance by all team members.

4.5 FCC CIRT Process Summary



5 PREVENTING FUTURE DAMAGE TO FCC SYSTEMS

Once resolved, an incident can offer an invaluable educational experience for the FCC CIRT. Such efforts may prevent (or at least minimize) damage from future incidents. The CSO, CIRT members, and FCC management can study incidents internally to gain a better understanding of the Commission's threats and vulnerabilities so more effective safeguards can be implemented. Additionally, outside contacts (established by the platform group members) can provide early warnings of threats and vulnerabilities (e.g., a new computer virus traversing the Internet).

The incident handling capability allows FCC CIRT members to learn from the incidents that it has experienced. The CIRT can collect data about past incidents (and the corrective measures taken) and analyze the data for patterns. This analysis may include determination of which viruses are most prevalent, which corrective actions are most successful, and which systems and information are being targeted by hackers.

The CIRT can identify vulnerabilities in this process. For example, it may determine whether a new software package or patch introduces a vulnerability into an FCC system. Knowledge about the types of threats that are occurring and the presence of vulnerabilities can aid in identifying security solutions. This information will also prove useful in creating a more effective training and awareness program, and thus help reduce the potential for exposure.

6 TECHNICAL PLATFORM MEMBER EXPERTISE

The technical staff members who comprise the platform FCC CIRT teams need specific knowledge, skills, and abilities relevant to their respective operating systems and platforms. Knowledge of their systems is expected through the day-to-day administration and management of their systems.

7 FCC CIRT EDUCATION AND AWARENESS TRAINING

The CSO encourages all FCC CIRT members to keep up-to-date with available educational and training opportunities available in the areas of system management and related security with their respective systems. Further, the FCC CIRT can benefit from lessons learned during incident handling. CIRT staff will be able to help assess the level of user awareness about current threats and vulnerabilities and provide input for future training efforts. Staff members may be able to help train system administrators, system operators, and other users and systems personnel. Knowledge of security precautions (resulting from such training) helps reduce future incidents. Educational Computer Security Notices can increase system users understanding of the importance of reporting an incident.

8 FCC CIRT AND THE CONTINUITY OF OPERATIONS PLAN

Incident handling, by the FCC CIRT is closely related to COOP planning as well as support and operations. The FCC CIRT may be viewed as a component of contingency planning because it provides the ability to react quickly and efficiently to disruptions in normal processing. The FCC CIRT effort can be the FCC's last effort to avoid the necessity to invoke its COOP.

APPENDIX A: GLOSSARY

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.

Accreditation - A formal declaration by the designated approval authority that an information system is approved to operate using a prescribed set of safeguards at an approved level of risk.

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.

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

Application – Software used to provide a set of functionality and features to a set of users.

Auditing - Auditing is a security mechanism that tracks the actions of system users, administrators, and processes in order to provide traceability and accountability.

Audit Logs - Audit logs (also known as audit trails) are records in which the output of auditing mechanisms is stored for analysis and historical reference.

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

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.

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

Certification - Comprehensive evaluation of the technical and non-technical security features of an information system made in support of the accreditation process.

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

Continuity of Operations (COOP) – A predetermined set of instructions or procedures that describe how an organization's *essential functions* will be sustained for up to 30 days as a result of a disaster event before returning to normal operations.

Denial / Disruption of Service (DoS) - An attack on an information system that interferes with or disrupts the performance of the targeted information system.

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.

Encryption - A security mechanism that renders information unintelligible to unauthorized persons and allows the information to be restored to its plain-text format by authorized persons.

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.

Hacker - Colloquial term used to refer to persons who attempt to access information systems and network resources in an unauthorized manner.

Least Privilege - A security control that requires system users and computer processes to be granted the minimum level of privilege and access needed to perform their authorized duties and functions.

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.

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.

Network Service - A network service is a logical portion of the operating system used to communicate specific types of information among computers.

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.

Process - A process is a program in a state of execution, or a program that is running and has not finished.

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.

Risk - A combination of the likelihood that a negative event will occur and the severity of the impact of that event.

Segregation of Duties - Segregation of duties refers to the policies, procedures, and organizational structure that help ensure that one individual cannot independently control all key aspects of a process or computer-related operation and thereby conduct unauthorized actions or gain unauthorized access to assets or records without detection.

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.

System - A collection of hardware, software, operating system, and firmware integrated together to perform one or more functions.

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.

System Administration - The process of supporting and managing the use, configuration, functionality, and security of production information systems.

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

Vulnerability - A condition of security weakness in an information system that may be exploited by internal or external adversaries to cause a negative impact on the confidentiality, integrity, or availability of an information system.

APPENDIX B: REFERENCES

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."

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.

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.

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.

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.

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).

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.

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.

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.

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.

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.

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.

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.

FCC Directive FCCINSTR 1139, "Management of Non-Public Information." The purpose of this directive is to establish policies and procedures for managing and safeguarding non-public information.

FCC Directive FCCINSTR 1479.2, "FCC Computer Security Program." 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.

Prepared for:

Federal Communications Commission
Office of the Managing Director
Information Technology Center
Computer Security Program
445 12th Street, SW
Washington, D.C. 20554

Prepared by:

NETSEC
WWW.NETSEC.NET

GSA Schedule Contract Number: GS-35F-0040K