FCC Computer Security

Desk Reference

Identification and Authentication on FCC Computer Systems

Technical Control Guide No. TC-310

July 2002

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

TABLE OF CONTENTS

1 INTRODUCTION 1

1.1 PURPOSE 1
1.2 BACKGROUND 1
1.3 SCOPE 2
1.4 AUTHORITY 2

2 ROLES AND RESPONSIBILITIES 3

2.1 FCC USERS 3
2.2 SYSTEM ADMINISTRATORS / APPLICATION OWNERS 3
2.3 COMPUTER SECURITY OFFICER 4

3 ACCOUNT AND PASSWORD GUIDELINES 5

3.1 NON-PRIVILEGED, NON-ADMINISTRATIVE USER ACCOUNTS 5
3.2 PRIVILEGED, ADMINISTRATIVE ACCOUNTS 6

4 ADMINISTRATIVE AND EMERGENCY ACCESS GUIDELINES 9

4.1 ADMINISTRATIVE GUIDELINES 9
4.2 EMERGENCY ACCESS GUIDELINES 9

5 PERIODIC VALIDATION OF USER ACCESS AND ACCOUNT PRIVILEGES 10

6 ANNUAL PASSWORD TESTING 10

7 SPECIAL CASES 11

7.1 ROUTERS 12
7.2 SIMPLE NETWORK MANAGEMENT PROTOCOL 12

APPENDIX A: GLOSSARY 14

APPENDIX B: REFERENCES 16

1 INTRODUCTION

1.1 Purpose

The purpose of this guide is to provide security guidance and communicate procedures to Federal Communications Commission (FCC) employees to help ensure that Identification and Authentication (I&A) security mechanisms are properly managed and enforced on FCC systems. Specifically, this guide addresses the following areas of system administration and application management:

- Describes user responsibilities for selecting strong passwords and protecting passwords;
- Describes FCC requirements and guidelines for system developers to configure I&A controls during the development lifecycle;
- Provides security guidance to system administrators and application owners to ensure that I&A controls are properly managed over the production lifecycle of FCC systems; and,
- Identifies security guidelines and procedures to assist managers with ensuring the proper enforcement and management of I&A controls.

Note: Throughout this document, the term "system" denotes application(s), or an operating system, or a combination of both the operating system and application(s).

1.2 Background

To aid system administrators and application owners in performing effective security administration, the FCC Computer Security Office has developed security guidelines that implement FCC and Federal security directives and policies. This document, coupled with the FCC's other security policies and documentation, addresses the OMB Circular A-130, Appendix III requirement for 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."

I&A are security mechanisms designed to help enforce access control policies on information systems. The term *Identification* refers to the use of an identifier, such as a UserID, to associate a person/user with a set of access authorizations and privileges on a particular information system (i.e., an account).

While it is important to identify each user before granting access, a system must also establish a strong association between the person and the UserID. A system uses *Authentication* mechanisms, such as passwords, to establish the validity of the user's claimed identity.

I&A helps to provide confidentiality and integrity of data through access controls. It helps to prevent access by unauthorized users. It helps to prevent authorized system users from assuming unauthorized privileges. It helps the system associate a user with actions performed on the systems for purposes of accountability and auditing. Failure to enforce I&A controls can result in a potentially disastrous compromise of confidentiality, integrity, and availability of the system and its data.

1.3 Scope

The guidance contained in this document applies to users, system administrators, application managers, application owners, system developers, and system owners. This guidance applies 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. This includes personal computers, servers, routers, security devices (such as firewalls and intrusion-detection systems), e-filing applications, and software applications.

The guidelines in this document apply generally to all operating systems and applications in use at the FCC. However, not all applications and operating systems used at the FCC provide inherent security features to enforce all of the guidelines in this document. These guidelines should be enforced to the extent possible using the security features available on FCC systems. Where individual systems do not support these guidelines, system developers and administrators must consider other techniques, which may include policy, procedures, and supplemental security products.

1.4 Authority

This document is issued pursuant to the Computer Security Act of 1987; OMB Circular A-123; OMB Circular A-130; Government

Information Security Reform Act (Public Law 106-398); FCC Directive FCCINST 1479.2, and other related guidance.

2 ROLES AND RESPONSIBILITIES

2.1 FCC Users

Users of FCC systems play an important role in protecting sensitive systems from compromise. Users are responsible for adhering to the following practices regarding protection of accounts and passwords used to access FCC information systems.

- Users must select strong passwords according to the guidelines in this document and FCC Instruction 1479.2 (i.e., not the same or reverse as the UserID, not the user's name or initials, not words easily found in a dictionary, not words that are easily associated with the user, etc.)
- Users must never write their password down.
- Users must not share their passwords or account access with anyone. (Procedures for emergency and administrative access to user accounts are described later in this document.)
- Users must notify the Computer Resource Center and the Computer Security Officer if they believe that their FCC accounts or password has been compromised.
- Users are only authorized access to data and systems that are necessary to perform their job duties.
- Users must read and follow the security instructions in FCC Instruction 1479.2.

2.2 System Administrators / Application Owners

System administrators and application owners have the following security responsibilities for the systems that have been assigned to them.

- Maintain security over the operational life of a system by ensuring proper configuration according to this guideline and other FCC directives and policies.

- Ensure that user access to systems is properly granted, maintained, and revoked.
- Perform periodic reviews of user accounts to ensure that user privileges are in line with job responsibilities.
- Perform periodic reviews of user accounts to ensure that only authorized persons maintain access to the system. Any continued access should be granted on a "need-to-access" basis.
- Perform automated testing of general support systems and major application passwords to ensure adherence to this guide.

2.3 Computer Security Officer

The FCC Computer Security Officer is responsible for development of computer security policy and oversees information security operations at the FCC. Oversight of computer security operations includes the following responsibilities.

- Develop and disseminate security guidelines for use by system administrators and application owners.
- Conduct certification and accreditation of FCC systems prior to being placed into initial production and every three years thereafter, or when significant modifications are made to the system.
- Assist application owners with identifying, tracking, and resolving temporary accreditation issues before a system is placed into production and granted approval to operate.
- Ensure creation and maintenance of System Security Plans, as required by OMB Circular No. A-130, Appendix III.
- Provide security training and awareness to FCC information system users.
- Perform annual testing of passwords for major applications and general support systems.

3 ACCOUNT AND PASSWORD GUIDELINES

3.1 Non-Privileged, Non-Administrative User Accounts

Effective administration and management of user accounts is a core discipline for secure administration of information systems. The FCC's guidelines for account setup and management must be applied consistently to be effective. System developers, system administrators, and application owners must follow the guidelines listed below.

3.1.1 Account Guidelines

- The system must require each user to uniquely identify and successfully authenticate to gain access.
- Systems must not allow anonymous, guest, or shared account access unless explicitly authorized by the Computer Security Officer.
- UserID configuration will be set as the first character of the user's first name and the first seven characters of the user's last name (i.e., Jane Doe = jdoe).
- The system must use the standard UserID assigned to FCC system users to access FCC computer systems. Users must not have different account IDs across more than one system.
- The system must prevent initiation of concurrent, non-administrative, user logins to access FCC production systems, unless otherwise approved by the CSO.
- No user account may have the same UserID as another user on the system.
- The system must disable a user's account after three consecutive failed login attempts. Once disabled, the account must be locked from access and scheduled to reset automatically after 15 minutes.
- The system must invoke a password-protected screen saver after not more than 10 minutes of inactivity. The system must provide direct users the ability to invoke a password-protected screen saver.

3.1.2 Password Guidelines

- Users must select strong passwords that are not the same or reverse as the UserID, not the user's name or initials, not words easily found in a dictionary, etc.
- The system must enforce minimum password length of 6 characters using a combination of alphanumeric, lower and upper cases letters, and special characters. At least one character of the password must be a numeric, upper case, or special character.
- The system must enforce password aging by requiring users to change passwords at least once every 90 days.
- The system must enforce uniqueness of the previous four passwords; passwords may only be used once in a twelve month period.
- The system must give users at least five days of warning before their password expires.
- The system must require new users to change their password after the first use of their account and after the password has been reset to a default password.
- If using automated login scripts for system access, the script must not contain the user's login password.
- Compromised passwords must be invalidated immediately upon detection of the compromise and a new password issued.
- The system must encrypt passwords during storage on a system.
- Before placing a system into a production environment, system administrators must change all default passwords and all passwords that were used in the development environment. They must also document the fact that they changed the passwords.

3.2 Privileged, Administrative Accounts

Administrative accounts and their passwords are highly sensitive, non-public information and must be carefully protected against disclosure. These accounts, in many cases, have the ability to access,

change or delete almost all files on a system. They have the ability to execute sensitive programs, install hardware and software, and make changes to the operating systems and applications. Gaining access to these accounts is the primary goal of "hackers" because it gives them the keys to the system and its data.

In addition to the guidelines for non-privileges accounts and passwords, system administrators, application owners, and system developers also must follow the guidance in the sections below for privileged, administrative accounts.

3.2.1 Account Guidelines

In addition to requirements for management of non-administrative accounts, the following requirements apply to privileged, administrative accounts.

- The system must require login under a non-privileged account ID before executing a command to upgrade access to the privileged, administrative account. The goal is to ensure that each user is accountable for his or her actions by ensuring that actions can be associated with an authenticated UserID. Login under system and administrative accounts allows actions to be performed on the system that are not associated with an individual user.
- Restrict privileged, administrative passwords to the minimum required number of personnel. The manager of the organization responsible for the system must maintain a list of personnel who are authorized to gain administrative access to systems under his / her control.

3.2.2 Password Guidelines

In addition to requirements for management of non-administrative passwords, the following requirements apply to privileged, administrative passwords.

- The system must prompt for a change of the administrative password at least every 60 days.
- Each system must have a unique administrative password. It is bad security practice to set the administrative password to be the same on multiple systems.

- Administrative passwords must not be passed in clear text across an internal FCC network or an external network.
- System administrators must change the administrative password when they revoke an administrative user's access to the administrative / superuser account.
- The system must enforce uniqueness of the previous six passwords on administrative accounts, such that administrative users may use a password only once in a twelve month period.
- Prior to a system being put into production, default passwords must be changed and documented.

3.2.3 Archiving Privileged, Administrative Passwords

Loss or compromise of the administrative passwords (such as root or superuser) for a system can result in severe consequences. If the password is forgotten or if only one person knows the password and that person is no longer accessible, administrators may have to re-install the system to restore administrative access. Similarly, mishandling the administrative password can result in compromise of a system.

As a result, careful precautions will help to prevent loss and compromise of the administrative/privileged password(s). Each organization that is responsible for administering systems that process sensitive data must enact procedures for the secure archival and retrieval of administrative passwords in cases of emergency. The guidelines are as follows.

- A copy of the current administrative password(s) for each system must be archived in a physically secure location that prevents undetected and unauthorized access to the password (for example, in a dated, signed & sealed envelope stored in an operational electronic-media safe).
- The administrative password archive must be under the control of the organization's manager. This archived password is for emergency use only. The manager must authorize and track access to the archived password under emergency procedures.

- The administrative password must be changed immediately after emergency access to the archived password.

4 ADMINISTRATIVE AND EMERGENCY ACCESS GUIDELINES

The guidelines in the sections below apply to situations where system administrators and Computer Resource Center (CRC) personnel must change user passwords or access a user's account.

4.1 Administrative Guidelines

- Users who forget their password will report to the CRC and show their badge for proper identification prior to the CRC resetting their password.
- When regional and field-office users require their password to be re-set, they may contact the CRC by phone to make the request. CRC staff must verify the employee's FCC phone number using a source such as the FCC phone book and call the employee back at the verified number before resetting the password.
- Compromised passwords must be invalidated immediately upon detection or notification of the compromise and a new password issued. If suspicious activity is suspected, the account will be locked to prevent user access in coordination with the Computer Security Officer.
- Computer Resource Center personnel, FCC managers, system administrators, application owners, and other FCC employees are ***not*** authorized to request an FCC user to reveal his or her password.

4.2 Emergency Access Guidelines

- In cases where management requires access to a user's account, the password must be reset to facilitate access. Management will ***not*** obtain access by requesting that the user reveal his or her password.
- If the user's access to his/her account must be restored

after managerial access or after the password has been reset to a default password, the system must prompt the user to change the password upon first login.

- If the system does not prompt the user to change his or her password from the default, the user must ensure that the password for the account is reset.

5 PERIODIC VALIDATION OF USER ACCESS AND ACCOUNT PRIVILEGES

Application owners and system administrators are responsible for performing a review of user accounts at least once every six months. This applies to operating systems and applications. The application owner or the system administrator must review the list of user accounts to ensure that the following guidelines are applied.

- All users of the system must have a current business need to access the system according to their current job duties.
- System administrators must identify accounts that have been inactive for 45 days or more and validate the business need for that account by contacting the manager of the business area supported by the system. Administrators must delete the account if the user is no longer employed or contracted by FCC or if the user no longer has a valid business need to access the system.
- The level of access and privileges granted to the account must be appropriate for the job duties of the user. Administrators must carefully scrutinize accounts with higher levels of privilege to ensure that the user has a valid business need for the additional privileges.
- The person who performs the review must generate a printout of the current, valid user accounts. That person must sign and date the printout and maintain a copy for one year as evidence of the review.

6 ANNUAL PASSWORD TESTING

The Computer Security Officer's staff will perform annual automated security testing of passwords on general support systems and major

applications (as defined by OMB Circular A-130, Appendix III). The CSO's staff will perform the tests during the annual agency program review (also known as "agency self-assessments") that is required by the Government Information Security Reform Act (GISRA) (Title X, subtitle G of Public Law 106-398).

System administrators and application owners must assist the CSO's staff, which may request access to password files for applications and operating systems. The CSO's staff will report the findings to systems personnel who must create an action plan to address any findings.

The purpose of the test is to verify that users and administrators follow the guidelines outlined in this document for selection of passwords. The tests will search for passwords that are common dictionary words, UserIDs, user names, and blank passwords that may be obtained through common guessing attempts. The CSO's staff will use automated tools that are appropriate for the system being tested.

The tests typically will not involve an exhaustive analysis designed to recover all passwords. Such tests are time and processor intensive, can adversely impact system performance, and may require weeks or months of continuous processing to complete.

On systems that allow the encrypted password file to be copied to a file, the CSO's staff will perform the tests in their office. On systems where the password file may not be copied to a file, the CSO's staff will perform tests on the system itself. In that case, tests will be scheduled around critical operations to minimize impact on system performance. During testing, operational passwords will be disclosed only to authorized personnel. Disclosed passwords must be changed immediately after conclusion of the tests.

For more information on OMB Circular A-130, Appendix III, GISRA, and the responsibilities of system administrators and applications owners, please see *FCC Computer Security Desk Reference Guide Number MC-110, "Security Guide for Application and System Management."*

7 SPECIAL CASES

Some devices and protocols require additional security procedures or protections to ensure that I&A is implemented securely. The following sections discuss I&A issues related to two special cases.

7.1 Routers

In addition to I&A guidelines listed throughout this document, router administrators must apply unique protections to I&A mechanisms on routers. The guidelines listed below primarily apply to Cisco routers, which is the most prevalent brand of router currently used at the FCC.

- All local (i.e. console) and remote access to routers must be authenticated; stronger authentication mechanisms such as Kerberos, TACACS+, Radius, or one-time passwords must be used where available.
- Each device must have a unique "enable" password; the same "enable" password may not be used on two or more devices.
- Passwords and all remote accesses must be encrypted in transit across a network. This includes internal FCC networks, non-FCC networks, and network connections/links between FCC networks. It applies to all methods of remote access to routers.
- Administrators must enable *Service Password Encryption* on routers.
- The strongest available option for encryption and hashing algorithms must be used to protect enable passwords; the basic *enable password* feature does not provide adequate protection.

For additional security guidance related to routers and network devices, please see *FCC Computer Security Desk Reference Number TC-340, "FCC Router and Firewall Administration Guide"*.

7.2 Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is a communications protocol used to pass management and configuration data among operating systems, applications, and system management software. It is commonly used to centrally monitor and manage the health, performance, and configuration of systems deployed across a distributed environment.

SNMP carries I&A data between systems in the form of "community strings," which are similar to passwords and must be protected like passwords. An adversary who is able to capture community strings

from SNMP data passed across a network may be able to gain unauthorized administrative access to critical network devices.

System administrators must follow the guidelines listed below when configuring community strings on SNMP-managed FCC systems.

- Replace default community strings values with values that meet the password guidelines presented in this document.
- Use SNMP version 3.0 or later, which provides stronger security mechanisms for the protection of community strings than previous versions of SNMP.
- Set community strings to *Read Only* to prevent modification by unauthorized persons.
- Encrypt community strings that are transmitted across a network using the strongest available encryption. This includes internal FCC networks, non-FCC networks, and network connections/links between FCC networks.

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.

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*, which 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.

Authentication - Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.

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

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

General Support Systems - 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.

Identification - The use of an identifier, such as a UserID, to allow an information system to associate a person/user with a set of access authorizations and privileges on a particular information system.

Password - A unique, secret, string of alphanumeric characters selected by each user that is associated with a particular UserID. The password's 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.

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.

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

UserID - The authorization code used to identify FCC users who are entitled to access FCC computer resources.

APPENDIX B: REFERENCES

Public Law 99-474: "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: "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: "Internal Control Systems." Requires heads of government agencies to 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: "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 USC 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:

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