BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE MANUAL 33-223

1 JUNE 1998

Communications and Information

IDENTIFICATION AND AUTHENTICATION

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the SAF/AAD WWW site at: http://afpubs.hq.af.mil. If you lack access, contact your Publishing Distribution Office (PDO).

OPR: HQ AFCA/GCI (MSgt Kaiser)
Certified by: HQ USAF/SCXX (Lt Col Webb)
Supersedes AFSSI 5013, 1 July 1996.
Pages: 16
Distribution: F

This Air Force manual (AFMAN) implements Department of Defense Directive (DoDD) 5200.28, *Security Requirements for Automated Information Systems (AISs)*, March 21, 1988; Department of Defense Manual (DoDM) 5200.28, *ADP Security Manual*, January 1973; Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*; Public Law 100-235, *Computer Security Act of 1987*; and Air Force Policy Directive (AFPD) 33-2, *Information Protection*. It relates to Air Force Systems Security Instruction (AFSSI) 5102, *The Computer Security (COMPUSEC) Program* (will convert to Air Force Instruction [AFI] 33-202*)*. It provides identification and authentication computer security requirements for operational information systems. Send recommended changes or comments to Headquarters Air Force Communications Agency (HQ AFCA/XPXP), 203 W. Losey Street, Room 1060, Scott AFB IL 62225-5233, through appropriate channels, using AF Form 847, **Recommendation for Change of Publications**, with an information copy to HQ AFCA/GCI, 203 W. Losey Street, Room 2040, Scott AFB IL 62225-5234, and Headquarters Air Force Communications and Information Center (HQ AFCIC/SYNI), 1250 Air Force Pentagon, Washington DC 20330-1250.

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed. Unlike its predecessor, this publication is directive in nature. It targets key personnel (information system users, system administrators, workgroup managers, and computer systems security officers [CSSO]) most involved in identification and authentication. It updates procedures, and strengthens minimally acceptable password criteria.

Chapter 1

GENERAL INFORMATION

1.1. Purpose. This manual provides information system users, system administrators, workgroup managers, and CSSOs with proper identification and authentication (I&A) procedures. "Identification" is the process where individuals identify themselves to a system as a valid user. "Authentication" is the procedure where the system verifies the user has a right to access the system. User identifications (user-ID) and passwords, because of their cost-efficiency and ease of implementation, are the most common I&A method. Because of their vulnerability to interception or inadvertent disclosure, they are also the weakest of I&A methods. Passwords are only effective when used properly. Inappropriate passwords create some of today's most common information system vulnerabilities.

1.2. Glossary of References and Supporting Information. See **Attachment 1** and AFMAN 33-270, *Command, Control, Communications, and Computer (C4) Systems Security Glossary*.

1.3. Applicability. This manual applies to operational Air Force information systems using I&A techniques and supports the individual accountability requirement established in AFSSI 5102. **If there is a conflict between this AFMAN and another more specialized document, the more specialized document takes precedence (i.e., documents governing Sensitive Compartmented Information systems).** Specific criteria established in this AFMAN not incorporated due to technical, procedural, or feasibility constraints shall be identified in the system certification and accreditation documentation and approved/ disapproved by the designated approving authority (DAA).

1.4. Relationship to Other Publications:

1.4.1. AFSSI 5102 defines the password as a method of authentication to support accountability and access control.

1.4.2. CSC-STD-002-85, *Department of Defense Password Management Guideline Yellow Book*, provides a set of practices related to using password-based user authentication mechanisms.

1.4.3. AFSSM 5010, *Computer Security in the Acquisition Life Cycle*(will convert to AFMAN 33-226), provides guidance on password management during system acquisition and development.

1.4.4. AFMAN 33-229, *Controlled Access Protection (CAP)*, provides technical and procedural options for implementing controlled access protection.

1.4.5. NCSC-TG-017, *A Guide to Understanding Identification & Authentication in Trusted Systems*, provides guidance on designing and incorporating effective identification and authentication mechanisms.

1.4.6. Federal Information Processing Standards (FIPS) Publication 48, *Guideline on Evaluation of Techniques for Automated Personal Identification*, discusses techniques for the identification of individuals for the purpose of controlling access to computer networks.

1.4.7. FIPS Publication 83, *Guideline on User Authentication Techniques for Computer Network Access Control*, provides information and guidance on techniques and practices used to control access to computer resources via remote terminals and networks.

1.5. Responsibility. System administrators or workgroup managers (hereafter referred to as system administrators) are responsible for establishing and maintaining the I&A management program for the system; creating, distributing, controlling, and deleting identifiers and passwords; and maintaining the criteria outlined in this manual. Should mission requirements dictate, assign CSSOs to assist system administrators in I&A management.

Chapter 2

IDENTIFICATION AND AUTHENTICATION ISSUANCE PROCEDURES

2.1. Introduction. The system administrators follow procedures contained in this chapter when issuing information system passwords.

2.2. Initial Assignment. Prior to issuing passwords and user-IDs, make sure the user has taken appropriate computer based training according to AFI 33-204, *Information Protection Security Awareness, Training and Education (SATE) Program*. Make sure the user is briefed on the importance of protecting their user-ID and password; reporting any suspicious activity; fraud, waste, and abuse; and the use of system monitoring.

2.2.1. Organizations make sure a method is in place to authenticate requests for information system access before issuing passwords.

2.2.2. DAAs may require formal documentation for classified system requests. Use NSA Form G6521, **Access Request and Verification,** National Stock Number 7540-FM-001-34482; the AF Form 310, **Document Receipt and Destruction Certificate,** or a locally prescribed form/letter.

2.3. Password Generation. Use passwords generated by the information system or require users to generate their own password.

2.3.1. Adhere to requirements in CSC-STD-002-85 to meet an acceptable information system-generated password algorithm.

2.3.2. Passwords generated by the user must meet the criteria outlined in this publication. **Attachment 2** contains a sample password system interface that can be implemented by the system administrator to help users generate their own passwords.

2.4. Password Composition. Use passwords with at least eight alphanumeric characters (upper and lower case) with at least one special character (@&+, etc.). **Attachment 3** provides tips for effective password composition. Never make a password related to one's own personal identity, history, or environment. Modify systems unable to support eight character passwords at the earliest and most cost-effective opportunity. In the interim, use the maximum number of characters the system is capable of supporting.

2.5. Generic Passwords. Generic password assignment is prohibited (e.g., a system having "welcome" as the password for all newly created accounts) unless the user is required to change the password upon initial assignment.

2.6. Password Aging and Management. Change passwords every 90 days.

2.6.1. Establish a 6-month minimum password age on the system to prevent users from using former passwords.

2.6.2. Limit the number of attempts allowed for correct password entry. Set the degree of password entry protection and the number of allowed entry attempts according to the sensitivity of the protected data. Normally three attempts are permitted.

2.6.3. When the maximum amount of password attempts is exceeded, lock out the user-ID and/or terminal from use. Make sure this procedure cannot be defeated by a user or be used to cause a denial of service by locking out all user-IDs or terminals. Make sure procedures are in place so the user must request access reinstatement from the system administrator.

2.7. User-ID Uniqueness. Keep user-IDs unique and assign them to only one person. Do not reissue a user-ID to another person for 1 year after its previous deletion.

2.7.1. On systems with a high user turnover, such as in a training organization, the system administrator may substitute generic user-IDs (stuDent1, stuDent2, caDet001, caDet002, etc.) for user unique IDs. In this case, the system administrator must incorporate a tracking method to match individual students to generic user-IDs (log sheet, etc.). Once the student no longer requires access (new module, class graduation, etc.), cancel the passwords.

2.7.2. Occasionally, concerns about mission accomplishment necessitate using group user-IDs and passwords. System administrators allowing group accounts and passwords must maintain individual accountability. A manual solution is to require account users to denote access date and time on a log sheet.

Chapter 3

IDENTIFICATION AND AUTHENTICATION PROTECTION PROCEDURES

3.1. Introduction. System administrators and users will follow the policy contained in this chapter, as applicable, to control password disclosure.

3.2. Password Protection. Each user is responsible and accountable for their own password.

3.2.1. Memorize your password. Do not place passwords on desks, walls, sides of terminals or store them in a function key, log-in script, or the communications software. If documentation is necessary for mission accomplishment (i.e., pre-established accounts for contingency or exercise), place the password in a safe.

3.2.2. Users must enter their identifier and password upon initial access to an information system. A user must enter a password in such a manner that the password is not revealed to anyone observing the entry process.

3.2.3. Do not share your password. If password sharing is necessary for mission accomplishment make sure the password is changed immediately after shared access is no longer required.

3.2.4. Adhere to password composition requirements in paragraph 2.1.3.

3.3. Password Classification. All passwords must be protected based on the sensitivity of the information or critical operations they protect (i.e., a password used to gain access to a SECRET network is itself classified SECRET). At a minimum, you must safeguard all passwords as "For Official Use Only" (FOUO). See AFI 37-131, *Freedom of Information Act Program* (will convert to AFI 33-331), for an explanation of FOUO. User-IDs are an unclassified reference to a user that can be displayed on printouts and in audit trails without compromising the password.

3.4. Password Transmission. Protect passwords during transmission at the same level required for the system or data that the password is protecting. Passwords are typically sent for authentication from a terminal to the system by a communications line. Unless the line is physically protected or encrypted, the password is vulnerable to disclosure by wiretapping and/or sniffers. Prevent this vulnerability by electronic protection or password encryption. Increasing the password length and changing it more often can mitigate this vulnerability.

3.5. Unattended Workstations. Never leave the information system unprotected while “logged in.” Enable the system’s password protected screen saver (if so equipped) and/or employ physical measures (e.g., keyboard locks) before leaving the information system unattended.

3.6. Password Change Authorization. Users may use an established procedure to change their own password whether it is machine or user generated. The user must enter the old password and authenticate as part of the password change procedure.

3.6.1. If the user forgets the password, the system administrator must authenticate the user’s identity before changing the password.

3.6.2. If given a generic password (e.g., “password”), the system must prompt the user to immediately change to a new password. If the system is incapable of such a function, the system administrator must walk the user through the password change procedure.

3.7. Multiple Accounts. Use one of these three options if users require access to multiple systems:

3.7.1. Option 1: A different user-ID but same password for all systems.

3.7.2. Option 2: The same user-ID but different password for all systems.

3.7.3. Option 3: A different user-ID and different password for all systems.

Chapter 4

IDENTIFICATION AND AUTHENTICATION MAINTENANCE AND MANAGEMENT RESPONSIBILITIES

4.1. Introduction. System administrators will followthe policy contained in this chapter.

4.2. Deleting Default Accounts. Delete all unnecessary accounts and change all passwords included in a newly acquired system (software or hardware) before allowing any user access to the system. Many hardware components, such as servers, routers, and other networking devices come from the vendor installed with a few standard user-IDs (such as SYSTEM, TEST, MASTER, etc.) and passwords.

4.3. Deleting User Accounts and Passwords. Remove user-IDs and passwords from an information system whenever the user is permanently transferred to another location or terminates employment.

4.3.1. If a user is suspended from work or system access for any reason, remove or change the user-ID and password immediately.

4.3.2. Change a suspected or confirmed compromised password immediately.

4.4. Maintaining User Accounts. Review user-ID and password access to systems every 6 months to help identify dormant user-IDs and passwords.

4.4.1. Delete, expire, suspend, or change user-IDs and passwords as appropriate.

4.4.2. Make sure procedures are in place so the user must request access reinstatement from the system administrator.

4.5. System Configuration. Enable or configure the following information system features, if technically possible:

4.5.1. Configure the system to prevent rapid retries when entering a password incorrectly by allowing several seconds to elapse before requesting another password. This delay deters any automated, high speed, trial-and-error attack on the password system.

4.5.2. Following a successful log-in procedure, inform the user of the last successful access to the account and of any unsuccessful intervening access attempts. This aids in uncovering any unauthorized or attempted accesses that may have occurred.

4.5.3. Automatically log a user off the system if the workstation is inactive for a period of time.

4.5.4. Require user reauthentication to an inactive terminal on a periodic basis in addition to the initial authentication process.

4.6. Audit Trails. System administrators must ensure the system's audit trail function (when present) is enabled as directed in AFSSI 5102. The audit trail contains a record of successful and unsuccessful log-in attempts, file system modifications, change in privileges, and other data critical to the system's operation and security. The audit trail should not contain unencrypted (clear text) passwords, incorrectly entered passwords, or character strings, since this could expose the password of a legitimate user who mistakenly types the user-ID or password. The system may provide certain audit reports (for example, date and time

of last log-in) directly to the user. This allows the user to determine if someone else has used the account. Only authorized personnel, such as the system administrator, must have access to the audit trail file.

4.7. Security Tools. To the fullest extent possible, system administrators use security tools to provide the best defense against poor passwords. To accomplish this on UNIX-based systems, the Air Force Computer Emergency Response Team (AFCERT) has the following programs available:

4.7.1. Crack. This password cracking utility is designed to find weak or easily guessable passwords. Crack uses password rules in conjunction with defined dictionaries to guess encrypted passwords. Special dictionaries contain foreign words, mythological creatures, names, and cities/states/countries and are available via the Internet. Run Crack at least once a month to help enforce a strong password policy.

4.7.2. Computer Oracle Password and Security (COPS). COPS contains about a dozen different programs that attempt to counter common UNIX security problems. COPS checks for file permissions and modes and performs cyclic redundancy checks to ensure binary integrity. It can check for null passwords and poor passwords if a dictionary is identified, security of password and group files, and account integrity. Examine operating system networking files for vulnerabilities including the network configuration files. COPS also checks certain file dates and compares the dates to AFCERT advisory dates. This feature is a quick check to make sure the operating system is up-to-date with the known security holes and patches reported to AFCERT. COPS warns the system administrator of potential problems, but does not correct any of the problems it finds.

4.7.3. Security Profile Inspector (SPI) and Network Security Monitor (NSM). SPI and NSM identify security holes (vulnerabilities in operating system), check that security patches (recommended software fixes to an operating system and its applications) are installed and work correctly, check system file permissions, and monitor networks for malicious activity. SPI combines the functionality of programs such as COPS and TRIPWIRE (evaluates a system and checks for altered files, etc.). Its unique features include Access Control Test, Password Security Inspector, Binary Inspector, and Change Detector.

4.7.4. Crack, COPS, SPI, and NSM are part of the tools comprising the Base Information Protect collection of software. Additional information about these and other tools is available at the AFCERT web site.

Chapter 5

OTHER IDENTIFICATION AND AUTHENTICATION METHODS

5.1. Introduction. User-IDs and passwords are only one method available to identify and authenticate a user's identity. Passwords are popular because of their low cost; however, poor password use and management have left many systems vulnerable and are the key in the majority of system penetrations. This has encouraged the continued pursuit of more reliable methods. When necessary and appropriate, use other I&A methods as well.

5.2. Knowledge-Based. Knowledge-based I&A systems require the user to provide a pre-established piece of information in order to gain access. The authentication succeeds if the information provided by the user matches what the system expects. This approach is based on the concept that the user is the only one who knows what the computer expects and therefore is the person identified. This technique is vulnerable to attack by guessing or deducing the information. If the information is too simple or too easily associated with the person, it is more susceptible to hacker penetration. Examples of knowledge-based I&A include passwords, personal identification numbers (PIN), and other personal data. The user provides a unique piece of identification to the system; the system then prompts the user for that unique piece of information as an authenticator. This is by far the most common method used today to access an information system.

5.3. Possession-Based. Possession-based I&A systems require the user to produce a physical token that the system can recognize as belonging to a legitimate user. These tokens typically contain information physically, magnetically, or electrically coded in a form recognized by the host system. These systems reduce the threat from perpetrators who attempt to guess or steal passwords, because the perpetrator must either fabricate a counterfeit token or steal a valid token from a user. Examples of this technique include physical and electronic keys, challenge-response generators, smart cards (the Multilevel Information Systems Security Initiative uses FORTEZZA or FORTEZZA PLUS) and magnetic-strip cards or badges.

5.4. Biometric-Based. Biometric-based I&A systems rely on a unique physical characteristic to verify the identity of a user. Common identifiers include fingerprints, written signatures, voice patterns, typing patterns, retinal scans, and hand geometry. These authentication devices tend to cost more than knowledge- or possession-based systems, because the hardware required to capture and analyze physical characteristics is more complicated. However, these systems provide a very high level of security because the authentication is directly related to a user unique physical characteristic that is more difficult to counterfeit.

5.5. Combining Methods. One method that can substantially increase the security of an I&A system is to use a combination of I&A techniques. These techniques make it much more difficult for the perpetrator to obtain the necessary items for access. Automated teller machines have the most wide-spread use of this technique. The user must have a legitimate card with the correct information contained on the magnetic

strip as well as a PIN. Even if a perpetrator gets the card, they would need to guess or determine the PIN. This is why users are warned not to keep the PIN stored with the card.

WILLIAM J. DONAHUE, Lt General, USAF
Director, Communications and Information

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Public Law 100-235, *Computer Security Act of 1987*

CSC-STD-002-85, *Department of Defense Password Management Guideline Yellow Book*

NCSC-TG-017, *A Guide to Understanding Identification & Authentication in Trusted Systems*

FIPS Publication 48, *Guidelines on Evaluation of Techniques for Automated Personal Identification, April 1, 1977*

FIPS Publication 83, *Guideline on User Authentication Techniques for Computer Network Access Control, September 29, 1980*

OMB Circular, A-130, *Management of Federal Information Resources*

DoDD 5200.28, *Security Requirements for Automated Information Systems (AIS)*, March 21, 1998

DoDM 5200.28, *ADP Security Manual*, January 1973

AFPD 33-2, *Information Protection*

AFI 37-131, *Freedom of Information Act Program*

AFI 33-204, *Information Protection Security Awareness, Training, and Education (SATE) Program*

AFMAN 33-270, *Command, Control, Communications, and Computer (C4) Systems Security Glossary*

AFMAN 33-229, *Controlled Access Protection (CAP)*

AFSSM 5010, *Computer Security in the Acquisition Life Cycle* (will convert to AFMAN 33-226)

AFSSI 5102, *The Computer Security (COMPUSEC) Program* (will convert to AFI 33-202)

Abbreviations and Acronyms

ADP—Automatic Data Processing

HQ AFCA—Headquarters Air Force Communications Agency

HQ AFCIC—Headquarters Air Force Communications and Information Center

AFCERT—Air Force Computer Emergency Response Team

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

AFSSI—Air Force Systems Security Instruction

COPS—Computer Oracle Password and Security

CSSO—Computer Systems Security Officer

DAA—Designated Approving Authority

DoDD—Department of Defense Directive

DoDM—Department of Defense Manual

FIPS—Federal Information Processing Standards

FOUO—For Official Use Only

I&A—Identification & Authentication

NSM—Network Security Monitor

OMB—Office of Management and Budget

PIN—Personal Identification Number

SPI—Security Profile Inspector

User-ID—User Identification

Terms

Audit Trail—Chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event. **NOTE**: Audit trail may apply to information in an information system, to message routing in a communications system, or to the transfer of COMSEC material.

Authentication—Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

Designated Approving Authority (DAA)—An official with the authority to formally assume responsibility for operating an information system or network within a specified environment.

Identification—Process an information system uses to recognize an entity.

Information—Knowledge such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in media.

Information System—The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information.

Log-in—Procedure used to establish the identity of the user, and the levels of authorization and access permitted.

Password—Protected/private alphanumeric string used to authenticate an identity or to authorize access to data.

User Identification (User-ID)—Unique symbol or character string used by an information system to identify a specific user.

Attachment 2

SAMPLE PASSWORD SYSTEM INTERFACE

A2.1. Changing Password for Sample User-ID:

A2.1.1. Please provide current password for verification: (user types in password).

A2.1.2. For hints on choosing a good password, type a question mark (?) followed by the [RETURN] key at the 'New password' prompt. **NOTE**: The question mark will not appear on the screen when typed.

A2.1.3. New password (?=Help): (user types in a ?).

A2.1.4. Suggestions For Choosing A Good Password:

A2.1.4.1. Your password is the key to your account. It should be easy to remember, but very hard for someone else to guess.

A2.1.4.2. Do not use your user-ID, a name, a hobby, or a single dictionary word.

A2.1.4.3. Do not use your social security, telephone, or license plate numbers.

A2.1.4.4. Do use a mix of uppercase and lowercase letters and a special character- **Swim!3MileS**, **1golFer***, **2FORU&me**.

A2.1.4.5. Do misspell words or replace syllables with numbers and special characters- **1onderFul!**, **For2natE#**, **aPHORDit$**, **56sheVY+**, **bOOik4u<**.

A2.1.4.6. Do use 2 or 3 words together - **Ear2Knee+**, **IBignosE%**,**BAG4golf!**, **MaiL4You=**.

A2.1.4.7. Do use the first letter of each word in a sentence - "My three dear Daughters are very beautiful!" would become **M3dDavb!** and "My one son is a diligent worker" would become **M1siadw**.

A2.1.5. For hints on choosing a good password, type a question mark (?) followed by the [RETURN] key at the 'New password' prompt. **NOTE**: The question mark will not appear on the screen when typed.

A2.1.6. New password (?=Help): (user types in a password with 7 characters).

A2.1.7. Failed test - needs to be a minimum of 8 characters.

A2.1.8. For hints on choosing a good password, type a question mark (?) followed by the [RETURN] key at the 'New password' prompt. **NOTE:** The question mark will not appear on the screen when typed.

A2.1.9. New password (?=Help): (user types in lower, alphabetic password).

A2.1.10. Failed test - must contain at least one character from the following character sets: lower-case, uppercase, numeric, and special.

A2.1.11. For hints on choosing a good password, type a question mark (?) followed by the [RETURN] key at the 'New password' prompt. **NOTE**: The question mark will not appear on the screen when typed.

A2.1.12. New password (?=Help): (user types in good password).

A2.1.13. Passed test.

A2.1.14. Retype new password: (user correctly retypes good password).

A2.1.15. Match - new password implemented.

WARNING: Do not use the sample passwords in this document for actual passwords. They are probably already compromised and checked by hackers.

Attachment 3

PASSWORD MANAGEMENT QUICK REFERENCE SHEET

A3.1. The "DOs" of Password Management. Do:

A3.1.1. Use a combination of letters, numbers, and special characters.

A3.1.2. Mix the use of upper and lower case characters.

A3.1.3. Make the password pronounceable for easy memorization (for example, consonant-vowel-consonant).

A3.1.4. Use a length of eight or more characters in the password.

A3.1.5. Change your password every 60 to 90 days.

A3.1.6. Protect your password so you are the only one to know it.

A3.1.7. Enter the password carefully making sure nobody is watching.

A3.1.8. Use your account regularly to help you remember your password.

A3.1.9. Contact your CSSO if you suspect your password has been compromised.

A3.1.10. Make sure your password is not exposed on the screen during log-in.

A3.1.11. Verify the log-in information provided to make sure your account has not been used since your last session.

A3.2. The "DON'Ts" of Password Management. Don't:

A3.2.1. Use a single word by itself for the password; especially ones from the dictionary, slang words, names, or profanity.

A3.2.2. Use words personally associated with you.

A3.2.3. Write down your password unless absolutely necessary; if written, protect it so you are the only one who knows it.

A3.2.4. Store your password on the desk, wall, terminal or in a function key or the communications software.

A3.2.5. Share your password with anyone.

A3.2.6. Let anyone watch you enter your password.

A3.2.7. Leave your terminal unprotected while you are logged in.