



IDENTIFICATION AND AUTHENTICATION

"HOLDOVER"

"The basic publication has changed; impact on supplemental information is under review by the OPR. Users should follow supplemental information that remains unaffected."

NOTICE: This publication is available digitally on the AFDPO WWW site at:
<http://www.e-publishing.af.mil>

OPR: AFMC CSO/SCSN (Mrs. B. West)
Supersedes AFM 33-223/AFMCS 1,
30 December 1998

Certified by: AFMC CSO/SCS (Mr. P. Montanaro)
Pages: 8
Distribution: F

This supplement provides computer security requirements for identification and authentication on AFMC computer systems networks throughout their life cycle. It applies to all AFMC personnel who use, operate, or manage AFMC computer systems and facilities. It does not apply to the Air National Guard or US Air Force Reserve units and members. This supplement does not apply to classified systems.

SUMMARY OF REVISIONS

This supplement supersedes AFM 33-223/AFMC Sup 1, 30 December 1998.

AFMAN 33-223, 1 June 1998, is supplemented as follows:

1.3. This supplement applies to all AFMC systems using identification and authentication (I&A) criteria to support the individual accountability requirement established in AFSSI 5102, The Computer Security (COMPUSEC) Program, 23 Sep 96. This supplement is designed to provide guidance on I&A for all personnel that use and administer passwords.

2.2.3. (Added) Some systems will allow the users to independently change their own passwords. In other systems, changes are under central control. If users are allowed to generate their own passwords after the initial assignment by the Computer Systems Security Officer (CSSO) or designee, they must not use a password that is a one-syllable word, that is simple or familiar (such as, dictionary words), or family names. All users who change their own password must never use one that is related to their personal identity, history, or environment. The CSSO or designee must replace, not reissue passwords, forgotten by the users. The CSSO or designee must authenticate the user's identity before replacing the password.

2.4. In addition to the requirement of eight characters, it is suggested that passwords include at least one each uppercase and lowercase letters.

2.6. Passwords must be changed every 90 days, at a minimum, for all systems. Systems should have the capability to automatically prompt each user to change their expired password to implement this requirement.

2.6.4. (Added) In the case of a possible compromise or mishandling of the password, password must be changed within one workday. This includes inadvertently entering the password as the user-id.

3.2.5. (Added) Other methods can be used to protect passwords in storage.

3.2.5.1. (Added) Most systems have a password file that can be read only by the password system. The file is protected by a file access mechanism which checks a protection bit in a file access table. Only the authentication program has access to read the file and only the password change program has access to write to the file.

3.2.5.2. (Added) Some systems separate the password file from the authorized user file. An index file is used to provide the correspondence between the user and the user's password.

3.2.5.3. (Added) Computer terminals, push buttons, or password entry devices provide a means for minimizing the exposure of the password during entry. Where technically feasible, do not print the password on the terminal during the entry process. If unavoidable, a mask of characters should be printed on the terminal area for password entry. If the keyboard and the terminal display or printer are directly coupled, then mask the password by understriking the space where the password will be printed. Overstriking the area after the password entry may mask the password further. Do not use the same computer-generated masks every time to disguise the entered password. In any case, the password must not be displayed or printed after it has been entered. Passwords will not be programmed into function keys or any other automated function.

3.2.5.4. (Added) The cathode ray tube (CRT) terminals, which use half-duplex communications, may present a problem because the password overwrites the understriking and remains visible on the display. In such systems, the password system must immediately clear the display terminal after password entry. Users may manually clear the display terminal following password entry if the screen cannot be cleared by the password system.

3.2.6. (Added) Individual passwords are required for access to any system or network when the access is through dial-up modems. These are required in addition to the initial standard user identification (user-id)/passwords required for system access.

3.2.7. (Added) Contractor personnel are subject to access control procedures. Each contract requiring or allowing contractor personnel to have a user-id and password to access a computer, must include in the Statement of Work (SOW) the following requirements:

3.2.7.1. (Added) If the contractor requires access for the company's employees to government-owned computers, it shall request, through the prime contracting officer, assignment of a user-id and password. The request shall include the contractor or work order number, identification of the employee, including social security number, and shall identify whether or not the employee is a US citizen or whether application for citizenship has been made. If the employee is not a US citizen, any installation policies concerning foreign nationals accessing base network must be enforced. If no policy exists, the Foreign Disclosure Policy Office must approve a properly certified request. The request must include the employee's signature and a statement that the employee understands and accepts the requirement to personally protect any password assigned to him or her as a result of the computer access request.

3.2.7.2. (Added) The contractor must ensure that employees do not reveal their passwords to anyone. The obligation to enforce this requirement is a material element of the security requirements herein.

3.2.8. (Added) Ownership. Personal user-ids must be unique and assigned to only one person throughout the life cycle of the system. If a personal user-id is reused, it will not be reissued to another person for one year after its previous deletion. No two people will ever have the same personal user-id at the same time. Generic user-ids (i.e., scexec) are permitted because they are critical to function performed.

3.2.8.1. (Added) It should be considered a security violation when two or more people know the password for a personal user-id, except when the other person is the person assigned the duties of password management.

3.2.8.2. (Added) A user must be uniquely identified and authenticated by the system before taking any further action on the system. This is not intended to prohibit alternate forms of user identification (for example, group user-id) for nonauthentication purposes (for example: shared data access, mail).

3.2.8.3. (Added) The user can take one or a combination of several actions to prevent an observer from learning the password by watching the password entry process:

3.2.8.3.1. (Added) The users can use their bodies to prevent an observer from seeing the key being pressed during password entry.

3.2.8.3.2. (Added) The monitor's contrast or intensity can be turned down before entering the password and after entry waiting for the password to clear the screen before restoring the contrast or intensity.

3.2.8.3.3. (Added) The user can request a person or group not watch the password entry process.

3.2.8.3.4. (Added) The user can perform the password entry before allowing anyone into the area.

3.2.9. (Added) When submitted as part of a batch processing request, physically protect the password and add it to the request at the last possible moment. Batch processing requests submitted in punched cards must have the password card added by the user just prior to submission. The computer operations staff will maintain the card decks in a protected area and remove and destroy the password card after the deck has been read by the system. Never print the password on any output media. Onetime passwords distributed to the user in the form of a password list and sequentially used for sequential batch processing requests may be used; however, the lists must be physically protected by the user.

3.4. Do not provide passwords via the telephone unless a secure verification system has been developed. Do not provide passwords across the network via e-mail. Each user is responsible for changing their initial password immediately once access is gained to the new user account.

3.4.1. (Added) Password Dissemination. The user is first authorized the use of the computer system or accesses to a set of data, then an initial password is created and issued directly to the user. If passwords are generated centrally but are not delivered directly in person, they must be handled commensurate to the data they protect. There may be additional control points for systems with geographically separated remote processing sites or for networks. Passwords may be distributed in sealed envelopes marked, "To be opened by addressee only," and delivered to the users with clear instructions given to change the password immediately and destroy the contents of the envelope. Once the remote location receives the password, notify the system administrator, CSSO, or designee of its successful delivery and usage. A good method for detecting whether the password was compromised in distribution is to annotate the date and time the password was created and put into distribution to the user. Upon receiving the password, the user logs into the system, verifies that no access has been made to that account since the annotated time, and immedi-

ately changes the password. Another option is for the system administrator, CSSO, or designee to mark the password as expired and force the user to change the password before accessing the system. If the account has been accessed between creation and receipt, the user must immediately notify the system administrator, CSSO, or designee.

3.8. (Added) **Users' Authorizations/Password Revalidation.**

3.8.1. (Added) The users' authorizations must be revalidated at least annually or as determined by the DAA, system administrator, CSSO, or designee. Revalidation would also include the user's current office symbol, mailing address, and phone number. This will help to ensure that users who no longer require access or who have been reassigned, are deleted from the system. The user's supervisor must verify continued access to a system.

3.8.2. (Added) The person assigned the duties of password management must develop a procedure in which prompt notification is given when a user-id and password must be removed from the system. When a user is reassigned or no longer needs access to the system, delete the personal user-id and password, then change any group passwords associated with that user as soon as possible. The unit orderly room can assist in giving advance notice of reassignments. AFI 36-2102, *Base-Level Relocation Procedures*, 22Jun 98, prohibits using detailed out-processing checklists or establishing out-processing procedures that would require all personnel to process through activities where they are not obligated. However, AFI 36-2101, *Classifying Military Personnel (Officers and Airmen)*, 1 May 98, requires the military personnel flight (MPF) to produce a listing of impending relocation actions that can be used to identify individuals scheduled for out-processing. Notice of impending actions are not always optimal because those actions may be canceled or modified. It is best to establish a procedure where notification is provided as actions are completed or immediately thereafter. In addition, revalidate all user-ids periodically, and update information such as phone numbers and mailing addresses as necessary. This revalidation must be done at least once annually but may be performed more often as specified by the person assigned the duties of password management or higher level authority.

4.3.3. (Added) User procedures for each system must ensure removal of user's personal password and USERID by the end of the user's last duty day. This requirement should be part of the organization's out-processing checklist procedures and will apply to all civilian, military, and contractor personnel.

4.3.4. (Added) The password and associated user account must be disabled within 24 hours and deleted within ten workdays, or sooner, if specified by the system administrator, CSSO, or person assigned the duties of password management (designee) when:

4.3.4.1. (Added) The user leaves the organization. If the individual uses a group password to shared data, the group password must also be changed within three workdays.

4.3.4.2. (Added) The user no longer requires access for a period of greater than three months. This includes temporary duty travel and permanent or temporary organizational transfer. If the individual uses a group password to access shared data, the group password must also be changed.

4.3.4.3. (Added) An employee of a contractor or subcontractor is removed from work on a specific contract or task order, which requires access to the system or network. The contractor must notify the prime contracting officers as soon as possible, but within one workday of an employee's termination from work on a specific contract or task order.

4.6.1. (Added) The use of identification and authentication in the audit trail process includes: password creation; password expiration; use of password change procedures; the locking of a user-id; changes in privileges.

4.6.2. (Added) The person assigned the duties of password management must review audit trails and follow-up on all discrepancies commensurate with the sensitivity or criticality of the data being protected and the risk level of disruption or exploitation (for example: modems or network connectivity) to the system. Organization management as well as system administrator and other password management personnel must maintain and update system access records for all system users as changes occur (i.e. access request forms and listings including employee dismissal, retirement, and transfer). When these duties are performed or shared with private contractors or other DOD management organizations, management must insure these services are coordinated and understood in Service Level Agreements (SLAs), Statements of Work (SOW), Task Orders (TOs) and other official agreements. If the system is capable of generating an exception report, it is recommended that it be used for the review. For highly critical and sensitive systems, it is recommended that the review be performed on a daily basis. It must be ensured that the criteria outlined in **4.6.1. (Added)** are met.

4.6.3. (Added) Develop written procedures for each type of computer system. Assign user-id and password. As a minimum, this procedure should require completion of either AFMC Form 43, System Access Request or DISA Form 41, System Authorization Access Request. Either form is acceptable, but if access is requested on a non-DISA system, AFMC Form 43 would be the preferred form. **Attachment 4 (Added)** and **Attachment 5 (Added)** provide samples of AFMC Form 43 and DISA Form 41. When used, they should require approval by the individual's supervisor, or OPR of the data, password administrator, and the system security administrator. This also applies to all responsible personnel as described in **4.6.2. (Added)** In each case, the user will be required to sign the form specifying his or her agreement to ensure the protection of the password. The use of electronic signature is not authorized as part of this process until an approved methodology for verification has been developed. Do not provide passwords via telephone, unless a secure verification system has been established. Do not provide passwords across a network via e-mail.

Abbreviations and Acronyms (Added)

—included in AFMAN 33-223 under Abbreviations and Acronyms

Terms (Added)

Computer System Security Officer (CSSO)—Establishes and manages a computer security training program for information system (IS) users. Ensures users operate, maintain, and dispose of ISs according to security policies. Develops system security policy for ISs and networks that process or protect sensitive but unclassified information as well as those that process classified. Ensures security procedures are in place, i.e., practice of notifying CSSO (or alternate) if problems arise in regard to classified processing, viruses, etc. Performs initial evaluation of system vulnerabilities such as virus attacks and hacker intrusions; initiates and forwards reports for same to Base and MAJCOM Information Protection offices.

Attachment 5 (Added)

SAMPLE DISA FORM 41

Figure A5.1.

SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)			
PRIVACY ACT STATEMENT			
Public Law 99-474, the Computer Access Device and Computer Fraud and Abuse Act of 1984, authorizes collection of this information. The information will be used to verify that you are an authorized user of a Government automated information system (AIS) and/or to verify your level of Government security clearance. Although disclosure of the information is voluntary, failure to provide the information may impede or prevent the processing of your "System Authorization Access Request (SAAR)". Disclosure of records or the information contained herein may be specifically disclosed outside the DoD according to the "Blanket Routine Uses" set forth at the beginning of the DISA compilation of systems of records, published annually in the Federal Register, and the disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act.			
TYPE OF REQUEST <input type="checkbox"/> INITIAL <input type="checkbox"/> MODIFICATION <input type="checkbox"/> DELETION			DATE
PART I (To be completed by User)			
1. NAME (LAST, First, MI)		2. SOCIAL SECURITY NUMBER	
3. ORGANIZATION		4. OFFICE SYMBOL/DEPARTMENT	5. ACCOUNT CODE
6. JOB TITLE/FUNCTION		7. GRADE/RANK	8. PHONE (DSN)
STATEMENT OF ACCOUNTABILITY I understand my obligation to protect my password. I assume the responsibility for data and system I am granted access to. I will not exceed my authorized access.			
USER SIGNATURE			DATE
PART II (To be completed by User's Security Manager)			
9. CLEARANCE LEVEL	10. TYPE OF INVESTIGATION	11. DATE OF INVESTIGATION	
12. VERIFIED BY (Signature)		13. PHONE NUMBER	14. DATE
PART III (To be completed by User's Supervisor)			
15. ACCESS REQUIRED (Location) - Is DMC or BNC?			
16. ACCESS TO CLASSIFIED REQUIRED? <input type="checkbox"/> NO <input type="checkbox"/> YES	17. TYPE OF USER <input type="checkbox"/> FUNCTIONAL <input type="checkbox"/> SYSTEM	SECURITY ADMINISTRATOR APPLICATION DEVELOPER OTHER (specify)	
18. JUSTIFICATION FOR ACCESS			
VERIFICATION OF NEED TO KNOW I certify that this user requires access as requested in the performance of his/her job function.			
19. SIGNATURE OF SUPERVISOR		20. ORG./DEPT.	21. PHONE NUMBER
23. SIGNATURE OF FUNCTIONAL DATA OWNER/OPR		24. ORG./DEPT.	25. PHONE NUMBER
			22. DATE
			26. DATE
PART IV (To be completed by AIS Security Staff adding user)			
27. USERID (Mainframe)	28. USERID (Mid-Tier)	29. USERID (Network)	
30. SIGNATURE		31. PHONE NUMBER	32. DATE

DISA Form 41, SEP 1996 (EF)

DISA Form 41, SEP 1996 (EF)
Part Form V1.01

Figure A5.2.

PART V (Can be customized by DLEs or Customer with DLE approval (Optional)) (To be completed by User)	
33. ACCESS REQUESTED (Give specific system or application information)	
a. SYSTEMS)	b. DOMAINS)
c. SERVERS)	
d. APPLICATIONS)	
e. DIRECTORIES	
f. FILES	
g. DATASETS	
34. OPTIONAL USE	

DISA Form 41, SEP 1998 (EPI) DISA BC ICS, v.2
Form 41-01

DEBRA L. HALEY
Director, Communications and Information