FIPS PUB 112

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

1985 MAY 30

U.S. DEPARTMENT OF COMMERCE/National Bureau of Standards

PASSWORD USAGE

CATEGORY: ADP OPERATIONS
SUBCATEGORY: COMPUTER SECURITY

U.S. DEPARTMENT OF COMMERCE, Malcolm Baldrige, Secretary
NATIONAL BUREAU OF STANDARDS, Ernest Ambler, Director

Foreword

The Federal Information Processing Standards Publication Series of the National Bureau of Standards is the official publication relating to standards adopted and promulgated under the provisions of Public Law 89-306 (Brooks Act) and under Part 6 of Title 15, Code of Federal Regulations. These legislative and executive mandates have given the Secretary of Commerce important responsibilities for improving the utilization and management of computers and automatic data processing in the Federal Government. To carry out the Secretary's responsibilities, the NBS, through its Institute for Computer Sciences and Technology, provides leadership, technical guidance, and coordination of Government efforts in the development of guidelines and standards in these areas.

The need for physical, administrative, and technological measures to protect Federal information has become an acknowledged fact. Passwords and passphrases have become a commonly used measure to identify the authorized users of computer systems and, in some instances, to control access to data stored within a computer system. Passwords must be administratively controlled since they are issued to and known by people. Passwords must also be technologically controlled since they are stored in and processed by computers. This Standard and the Guidelines in the Appendices of the Standard establish fundamental administrative and technological controls for the proper usage of passwords. If the Standard and the Guidelines are followed properly, the security provided by a password security system will be enhanced.

James H. Burrows, Director Institute for Computer Sciences and Technology

Abstract

The document specifies basic security criteria for two different uses of passwords in an ADP system, (I) personal identity authentication and (2) data access authorization. It establishes the basic criteria for the design, implementation and use of a password system in those systems where passwords are used. It identifies fundamental ADP management functions pertaining to passwords and specifies some user actions required to satisfy these functions. In addition, it specifies several technical features which may be implemented in an ADP system in order to support a password system. An implementation schedule is established for compliance with the

Standard. Numerous guidelines are provided in the Appendices for managers and users seeking to comply with the Standard.

Key words: computer security; data security; passphrase; password; personal identification; systems security.

Natl. Bur. Stand. (U.S.) Fed. Info. Process. Stand. Pub. (FIPS PUB) 112, 55 pages (1985) CODEN:FIPPAT

For sale by the National Technical Information Service, U.S. Department of Commerce, Springfield. VA 22161.

FIPS PUB 112

Federal Information Processing Standards Publication 112

1985 May 30

Announcing the Standard for

PASSWORD USAGE

Federal Information Processing Standards Publications are issued by the National Bureau of Standards pursuant to section 111 (f) (2) of the Federal Property and Administrative Services Act of 1949, as amended, Public Law 89-306 (79 Stat. 1127), Executive Order 11717 (38 FR 12315, dated May 11, 1973), and Part 6 of Title 15 Code of Federal Regulations (CFR).

1. Name of Standard. Password Usage.

2. Category of Standard, ADP operations, computer security.

3. Explanation. A password is a sequence of characters that can be used for several authentication purposes. Passwords are often used to authenticate the identity of an automated data processing (ADP) system user and, in some instances, to grant or deny access to private or shared data. This Standard recognizes that passwords are not the only method of personal authentication, nor does it endorse the use of passwords as the best method; however, it recognizes that passwords are widely used in computer systems and networks for these purposes. In these systems and networks, compliance with this Standard will ensure that the passwords are used in accordance with accepted practices.
This Standard specifies basic security criteria for two different uses of passwords in an ADP system, (1) personal identity authentication and (2) data access authorization. A password used for personal identity authentication will be called a personal password; a password used for authorizing access will be called an access password. A personal password should not also be used as an access password. This Standard does not require the use of

passwords in an ADP system for either purpose, but establishes the basic criteria for the design, implementation and use of a password system in those systems where passwords are used.

This Standard identifies fundamental ADP management functions pertaining to passwords and specifies some user actions required to satisfy these functions. In addition, it specifies several technical features which may be implemented in an ADP system in order to support a password system. Those technical features desired by the ADP management should be specified in all procurement documents when acquiring new systems, and provisions should be made to ensure that they are included when upgrading existing systems. Technical features which are recommended for an ADP system are marked with an asterisk (*), In order to facilitate use of this Standard, this document includes explanatory and guideline appendices.

Some of the requirements of the Standard may be satisfied either through management functions or through technical features. For example, if the Security Officer specifies that each personal password is to be changed

at least every 6 months, the ADP manager can issue a directive to this effect or the ADP system can be programmed to automatically change a password 6 months after entry of its last change. This Standard does not specify how the criteria shall be met, but only what criteria shall be met. The technical features specified in the Standard are generally recommended, but cost considerations (costs to modify existing systems or additional operational costs) may require that management functions be utilized temporarily in satisfying the specified criteria.

4. Approving Authority. Secretary of Commerce.

5. Maintenance Agency. U.S. Department of Commerce, National Bureau of Standards, Institute for Computer Sciences and Technology.

The terms "secret" and "compromise" are used in this document in accordance with their dictionary definitions and do not imply National Security (Defense) related definitions. Use of cryptography to generate or transmit passwords for access to, or authentication of, classified information requires prior review and approval of the National Security Agency.

Export Control: Password systems incorporating cryptography and technical data regarding them are subject to Federal Government export control as specified in Title 22, Code of Federal Regulations, Parts 122 through 128. Software, firmware, and hardware incorporating cryptography and technical data regarding them must comply with these regulations.

10. Implementation Schedule. This Standard becomes effective June 1,1986.

11. Waivers. Heads of agencies may request that the requirements of this Standard be waived in instances where it can be clearly demonstrated that there are appreciable performance or cost advantages to be gained and when the overall interests of the Federal Government are best served by granting the requested waiver. Such waiver requests will be reviewed by and are subject to the approval of the Secretary of Commerce. The waiver request must specify anticipated performance and cost advantages in the justification for the waiver.

Forty-five days should be allowed for review and response by the Secretary of Commerce. Waiver requests shall be submitted to the Secretary of Commerce, Washington, DC 20230, and labeled as a Request for a Waiver to Federal Information Processing Standards Publication 112. No agency shall take any action to deviate from this Standard prior to the receipt of a waiver approval from the Secretary of Commerce.

12. Where to Obtain Copies. Copies of this publication are for sale by the National Technical Information Service, U.S. Department of Commerce, Springfield, VA 22161. When ordering, refer to Federal Information Processing Standards Publication 112 (FIPS PUB 112), and title. When microfiche is desired, this should be specified. Payment may be made by check, money order, or deposit account.

Federal Information
Processing Standards Publication
112

1985 May 30
Specifications for
PASSWORD USAGE

CONTENTS

Page

1.Terms and Conventions 8
1.1 Access Password 8
1.2 Authentication Process 8
1.3 Authorization Process 8
1.4 Compromise (Verb) 8

1.5 Cryptographic Key 8
1.6 Data 8
1.7 Data Encrypting Key 8
1.8 Encryption 8
1.9 Key Encrypting Key 8
1.10 Passphrase 8
1.11 Password System 9
1.12 Personal Identifier 9
1.13 Personal Password 9
1.14 Replace 9
1.15 Security Officer 9
1.16 System Manager 9
1.17 Valid Password 9
1.18 Virtual Password 9
2. Factors 9
2.1 Composition 9
2.2 Length Range 9
2.3 Lifetime 10
2.4 Source 10
2.5 Ownership 10
2.6 Distribution 10
2.7 Storage 10
2.8 Entry 10
2.9 Transmission 10
2.10 Authentication Period 10
3. Acceptable Basic Criteria 10
3.1 Composition 10
3.2 Length Range 11
3.3 Lifetime 11
3.4 Source 11
3.5 Ownership 12
3.6 Distribution 12
3.7 Storage 12
3.8 Entry 12

3.9 Transmission 13
3.10 Authentication Period 13

APPENDICES

APPENDIX A. PASSWORD USAGE GUIDELINES 14
1. Introduction 14
2. Background 14
3. Factors 14
3.1 Composition 15
3.2 Length 15
3.3 Lifetime 16
3.4 Source 17

3.5 Ownership 17
3.6 Distribution 17
3.7 Storage 18
3.8 Entry 19
3.9 Transmission 20
3. 10 Authentication Period 20
4. Examples of Password Systems 21
4. 1 Password System for Low Protection Requirements 21
4.2 Password System for Medium Protection Requirements 21
4.3 Password System for High Protection Requirements 22
APPENDIX B. EXAMPLES OF COMPLIANCE AND PROCUREMENT DOCUMENTS 23
1. Example of a Minimum Security Compliance Document 23
2. Example of a Procurement Specification for a Minimum Security Password System 24
3. Example of a Medium Security Compliance Document 24
4. Example of a Procurement Specification of a Medium Security Password System 25
APPENDIX C. 95-Character Graphic Subset from FIPS PUB 1-2 26
APPENDIX D. PASSWORD ENCRYPTION AND PASSPHRASE TRANSFORMATION 27
APPENDIX E. PASSWORD MANAGEMENT GUIDELINE 36
1. Introduction 36
2. Scope 36
3. Control Objectives 37
4. Definitions 37
5. Guidelines 38

5.1 SSO Responsibilities 38
5.1.1 Initial System Passwords 38
5.1.2 Initial Password Assignment 38
5.1.3 Password Change Authorization 39
5.1.4 Group IDs 39
5.1.5 User ID Revalidation 39
5.2 User Responsibilities 39
5.2.1 Security Awareness 39
5.2.2 Changing Passwords 39
5.2.3 Login to a Connected System 41
5.2.4 Remembering Passwords 41
5.3 Authentication Mechanism Functionality 41
5.3.1 Internal Storage of Passwords 41
5.3.2 Entry 41
5.3.3 Transmission 42
5.3.4 Login Attempt Rate 42
5.3.5 Auditing 42

5.4 Password Protection 43
5.4.1 Single Guess Probability 43
5.4.2 Password Distribution 43
APPENDIX E.1 PASSWORD GENERATION ALGORITHM 44
1. Password Space 44
2. Random Seeds 44
3. Pseudo-Random Number Generator 44
4. "User-Friendly" Passwords 45
APPENDIX E.2 PASSWORD ENCRYPTION ALGORITHM 46
1. Encryption Algorithm 46
2. Assurance for Unique Encrypted Passwords 46
APPENDIX E.3 DETERMINING PASSWORD LENGTH 47
1. Relationship 47
2. Guess Rate 47
3. Password Lifetime 48
4. Password Space 48
5. A Procedure For Determining Password Length 48
6. Worked Examples 49
7. Passphrases 50
APPENDIX E.4 PROTECTION BASIS FOR PASSWORDS 52
1. Systems Containing Only Unclassified Information 52
2. Systems Containing Classified Information 52
APPENDIX E.5 FEATURES FOR USE IN VERY SENSITIVE APPLICATIONS 53
1. One-Time Passwords 53
2. Failed Login Attempt Limits 53
APPENDIX E.6 ON THE PROBABILITY OF GUESSING A PASSWORD 54
APPENDIX E.7 REFERENCES 56

1. Terms and Conventions

The following terms or conventions and associated descriptions are used in the Standard.

1.1

Access Password

A password used to authorize access to data and distributed to all those who are authorized similar access to that data.

1.2

Authentication Process

The actions involving (1) obtaining an identifier and a personal password from an ADP system user; (2) comparing the entered password with the stored, valid password that was issued to, or selected by, the person associated with that identifier; and (3) authenticating the identity if the entered password and the stored password are the same. (Note: If the enciphered password is stored, the entered password must be enciphered and compared with the stored ciphertext or the ciphertext must be deciphered and compared with the entered password.)

1.3

Authorization Process

The actions involving (1) obtaining an access password from an ADP system user (whose identity has already been authenticated, perhaps using a personal password); (2) comparing the access password with the password associated with the protected data; and (3) authorizing access to the data if the entered password and the stored password are the same (see note above).

1.4 Compromise (Verb)

Disclosing a password, or part of a password, to someone not authorized to know, have or use the password.

1.5 Cryptographic Key

A parameter (e.g., a secret 64-bit number for DES) used by a cryptographic process that makes the process completely defined and usable only by those having that key.

1.6 Data

Programs, files or other information stored in, or processed by, a computer system.

1.7

Data Encrypting Key

A cryptographic key used for encrypting (and decrypting) data.

1.8

Encryption

The process of transforming data to an unintelligible form in such a way that the original data either cannot be obtained (one-way encryption) or cannot be obtained without using the inverse decryption process (two-way encryption).

1.9

Key Encrypting Key

A cryptographic key used for encrypting (and decrypting) data encrypting keys or other key encrypting keys.

1.10

Passphrase

A sequence of characters, longer than the acceptable length of a password, that is transformed by a password system into a virtual password of acceptable length.

1.11 Password System

A system that uses a password or passphrase to authenticate a person's identity or to authorize a person's access to data and which consists of a means for performing one or more of the following password operations: generation, distribution, entry, storage, authentication, replacement, encryption and/or decryption of pass-words.

1.12 Personal Identifier

A data item associated with a specific individual which represents the identity of that individual and may be known by other individuals.

1.13 Personal Password

A password that is known by only one person and is used to authenticate that person's identity.

1.14 Replace

To change a password to a different password selected from all possible acceptable passwords.

1.15 Security Officer

The ADP official, described in OMB Circular A-71, Transmittal Memorandum Number 1 (July 27,1978), having the designated responsibility for the security of an ADP system.

1.16 System Manager

The ADP official who is responsible for the operation of an ADP system.

1.17 Valid Password

A personal password that will authenticate the identity of an individual when presented to a password system or an access password that will allow the requested access when presented to a password system.

1.18 Virtual Password

A password computed from a passphrase that meets the requirements of password storage (e.g., 64 bits for DES).

2. Factors

The following basic factors shall be considered in the design, implementation, and use of a password system used to authenticate the identity of a person or to control access to data. The factors are:

2.1

Composition

Composition is the set of acceptable characters which may be used in a valid password.

2.2

Length Range

Length Range is the set of acceptable lengths of passwords, expressed as a minimum length through a maximum length (e.g., 4-8), i.e., all the acceptable number of characters in a valid password.

2.3 Lifetime

Lifetime is the maximum acceptable period of time for which a password is valid.

2.4 Source

Source is the set of acceptable entities which can create or select a valid password from among all acceptable passwords.

2.5 Ownership

Ownership is the set of individuals who are authorized to use a password.

2.6 Distribution

Distribution is the set of acceptable methods for providing (transporting) a new password to its owner and to all places where it will be needed in the password system.

2.7 Storage

Storage is the set of acceptable methods of storing a valid password during its lifetime.

2.8 Entry

Entry is the set of acceptable methods by which a password may be entered by an ADP user for authentication or authorization purposes.

2.9 Transmission

Transmission is the set of acceptable methods for communicating a password from its point of entry to its point of comparison with a stored, valid password.

2.10

Authentication Period

Authentication period is the maximum acceptable period between any initial authentication process and subsequent reauthentication processes during a single terminal session or during the period data is being accessed.

3. Acceptable Basic Criteria

A Password Standard Compliance Document shall be prepared by the Security Officer acting in conjunction with the ADP system manager which states for each selected factor, including the 10 basic factors: 1) the complete set of criteria to be satisfied; 2) the rationale for selecting the criteria; 3) the criteria to be satisfied with technical features implemented in the ADP password system; 4) the criteria to be satisfied through management functions and user actions. Only technical features required for an ADP password system should be included in procurement specifications. Technical features are noted below by an asterisk (*),

3.1Composition

3.1.1 Passwords shall be composed using a subset of characters selected by the System Manager and the Security Officer from the set of 95 graphics characters specified in FIPS PUB 1-2 and in Appendix C.

3.1.2 The subset shall not consist of less than 10 characters (e.g., the digits (k-9).

3.1.3 (*) An automated password system shall verify that only characters in the selected subset have been generated or selected whenever a password is created or changed.

3.2 Length Range

3.2.1 Passwords shall have a length range, selected by the System Manager and Security Officer, having a number greater than or equal to four (4) as the minimum length and a maximum length, based on, but not specified in, this Standard.

3.2.2 The selected password composition and length range shall allow for a minimum of 104 (10,000) possible passwords.

3.2.3 The selected password length range shall provide a level of protection commensurate to the value or sensitivity of the resources or data it protects.

3.2.4 Passphrases (i.e., passwords or encrypted passwords which cannot be stored in 64 bits) which are interchanged among ADP systems shall be transformed to a 64-bit virtual password (e.g., using the transformation algorithm specified in Appendix D) for storage.

3.2.5 (*) An automated password system shall verify that only passwords having a length within the acceptable length range shall be generated or selected whenever a password is created or changed.

3.3 Lifetime

3.3.1 Passwords shall have a maximum lifetime of 1 year.

3.3.2 Passwords shall have the shortest practical lifetime, selected by the Security Officer in conjunction with the Systems Manager, which provides the desired level of protection at the least possible cost (i.e., passwords should be changed often but only if the cost of replacement is reasonable and the owner is able to adopt the new password easily).

3.3.3 Passwords shall be replaced as quickly as possible but at least within 1 working day from the time that a compromise of the password is suspected or confirmed.

3.3.4 Passwords shall be deleted or replaced with an invalid password as quickly as possible but at least within 3 working days from the time that an owner is no longer an authorized ADP system user or any one of a set of owners is no longer authorized access to the data.

3.3.5 Passwords forgotten by their owner shall be replaced, not reissued.

3.3.6 (*) An automated password system shall allow the Security Officer to delete or replace a password (subsequent to authenticating the identity of the Security Officer).

3.3.7 (*) An automated password system shall have the capability of maintaining a record of when a password was created and changed.

3.4 Source

3.4.1 The source of passwords shall be selected by the Security Officer and the System Manager, and shall be one or more of the following: user, security officer, or automated password generator.

3.4.2 All passwords that may be included in a new system when it is delivered, transferred or installed (e.g., passwords for the operator, system programmer, maintenance personnel or Security Officer) shall be immediately changed by the Security Officer to: (a) passwords that are invalid to the password system; (b) random passwords that may be subsequently changed; or (c) valid passwords that are owned by authorized users of the system and created in accordance with this Standard.

3.4.3 Passwords that are created by the Security Officer for new users of the system during initial system access shall be selected at random from all acceptable passwords (i.e., default passwords or formatted passwords related to the new users identity or assignment shall not be used).

3.4.4 Users that create or select their own personal password shall be instructed to use a password selected from all acceptable passwords at random, if possible, or to select one that is not related to their personal identity, history or environment.

3.4.5 (*) Passwords selected or created by users or the Security Officer shall be tested by the automated password system to assure that they meet the specifications of composition and length established for the ADP system before they are accepted as valid passwords.

3.5 Ownership

3.5.1 Personal passwords used to authenticate identity shall be owned (i.e., known) only by the individual having that identity.

3.5.2 Access passwords used to protect private data shall be owned (i.e., known) only by the individual who created the private data.

3.5.3 Access passwords used to protect shared data shall be owned (i.e., known) only by the set of individuals authorized the same access privileges to that data.

3.5.4 The personal password of any individual who is authorized access to shared data, and the access password of that shared data shall not be intentionally selected or set to be identical.

3.5.5 Bach individual shall be responsible for providing protection against loss or disclosure to passwords in their possession.

3.6 Distribution

3.6. 1 Personal passwords shall be distributed from the password source in a way that only the intended owner may see or obtain the password.

3.6.2 Passwords shall be distributed in a way that an audit record, containing the date and time of a password change and the identifier associated with the password (but not the old or new password), can be made available to the Security Officer.

3.6.3 Passwords shall be distributed from the password source in such a way that temporary storage of the password is erased, and long-term retention of the password is available only to the owner(s) and the protected password system.

3.6.4 (*) An automated password system that generates and distributes passwords shall keep an automated record of the date and time of password generation and to whom it was distributed (but not the password itself).

3.7 Storage

3.7.1 (*) Stored passwords shall be protected in such a way that only the password system is authorized access to a password.

3.7.2 (*) Passwords that are encrypted before they are stored shall be protected from substitution (i.e., protection shall be provided such that one encrypted password cannot be replaced with another unless the replacement is authorized).

3.8 Entry

3.8.1 Passwords shall be entered by the owner when requested by the password system in a manner that protects the password from disclosure to anyone observing the entry process.

3.8.2 The number of allowed password entry attempts (retries after incorrect password entry) shall be limited to a number selected by the Security Officer.

3.8.3 The response to exceeding the maximum number of retries shall be specified by the Security Officer.

3.9 Transmission

3.9. 1 Passwords that are transmitted between the place of entry and the place that the entered password is compared with the stored password shall be protected to the degree specified by the Security Officer and at least equivalent to the protection required for the entity (ADP system or data) that the password is protecting.

3.9.2 (*) Passwords transmitted between the place of entry and the place of comparison with the stored password shall be encrypted at the place of entry if the data that the password is protecting are encrypted at the place of data entry.

3.9.3 (*) Passwords that are used as encryption keys shall be selected at random from the set of all possible keys (e.g., 236 keys for the DES) and shall be used either as Data Encrypting Keys or Key Encrypting Keys, but not both.

3.9.4 (*) Unencrypted passwords shall be transmitted as ASCII characters if interchanged between ADP systems; encrypted passwords and virtual passwords shall be transmitted either as a 64-bit binary field in bit-oriented communications, or as ASCII representations of the hexadecimal character set (i.e., the 16 characters in the set [0-9, A-F] in character-oriented communications).

3.10 Authentication Period

3.10.1 (*) Personal Passwords shall be authenticated each time a claim of identity is made, e.g., when "logging onto" an interactive system.

3.10.2 (*) Access passwords shall be authenticated during the initial request for access to protected data.

APPENDIX A

PASSWORD USAGE GUIDELINES

1. Introduction

This appendix contains background information, a discussion of the factors specified in the Password Usage Standard (herein called the Standard) and the rationale for the minimum criteria specified in the Standard. It also provides guidance in selecting parameters of password systems based on increasing security requirements. Examples of three password systems meeting increasing levels of security requirements are included.

2. Background

Passwords are the most common method of personal identification used in conjunction with remote terminals to deter unauthorized access to computer systems and networks. The effectiveness of passwords has often been questioned, primarily because they can be easily forgotten or given to another person. However, passwords can provide reasonable deterrence to unauthorized access if properly handled by people authorized to use them and if properly stored and processed in the password verification system. Within its Computer Security and Risk Management Program, the Institute for Computer Sciences and Technology of the National Bureau of Standards developed this Standard for secure password usage to assure reasonable handling, storage and processing of passwords. This Standard is one in a series of Standards and Guidelines issued by NEBS in the field of Computer Security. Another in this series, Federal Information Processing Standards Publication (FIPS PUB) 48, Guidelines on Evaluation of Techniques for Automated Personal Identification, describes various techniques for verifying identity and provides a set of criteria for the evaluation of automated identification systems embodying these techniques.

Shortly after issuing FIPS PUB 48, NEBS published Special Publication 500-9, The Use of Passwords for Controlled Access to Computer Resources. This publication considered the generation of passwords and their effective application to the problem of controlling access to computer resources. Following analysis and use of this document, a project was initiated to establish a fundamental performance standard for the use of passwords and a guideline on how to use this Standard to achieve the degree of protection that passwords were intended to provide.

The Password Usage Standard was developed within the Computer Security and Risk Management Program of the Institute for Computer Sciences and Technology with considerable assistance from representatives of Federal organizations and private industry. In 1980, NEBS developed and distributed a draft Password Usage Standard to government and industry representatives for comments and then held a workshop to discuss the benefits and impact of the draft Standard. The draft Standard identified 10 factors to be considered in the implementation of password systems and quantified security criteria in a hierarchical manner for each of the 10 factors. It also proposed five levels of security and specified minimum criteria for each level. The workshop participants felt that the 10 factors were useful in structuring the design of password systems, but that the proposed five levels were unworkable as a basis of a password Standard. As a result of the workshop recommendations, the Standard was revised to specify minimum criteria for the factors of a password system. An Appendix was drafted which provided guidelines for achieving higher levels of security. This revised Standard and the draft guidelines were published for public comment and for agency comment in July, 1981. The received comments were used in revising the proposed Standard and draft guidelines in preparing the published Standard and guidelines.

3. Factors

Ten factors of an automated password system are specified in the Standard. These factors constitute the fundamental elements which must be considered, specified and controlled when designing and operating a password system. The rationale for the factors and for the minimum acceptable criteria for the factors specified

in the Standard are provided in the following discussion. Guidance on how to meet the minimum criteria and reasons for exceeding the minimum criteria are also provided.

3.1 Composition

A password is a sequence of characters obtained by a selection or generation process from a set of acceptable passwords. A good password system has a very large set of acceptable passwords in order to prevent an unauthorized person (or intruder) from determining a valid password in some way other than learning it from an authorized person (i.e., owner). The set of acceptable passwords should be large enough to assure protection against searching and testing threats to the password system (and hence the data or resources that it protects) commensurate with the value of the data or resources that are being protected. The set of acceptable passwords must be such that it can be specified easily, that acceptable passwords can be generated or selected easily, that a valid password can be remembered, can be stored reasonably, and can be entered easily. Composition is defined as the set of characters which may comprise a valid password.

The composition of a password depends in part on the device from which the password is going to be entered. It also depends on how and where the password is going to be stored and how the stored password will be compared with the entered password. Federal Information Processing Standards Publication 1-2 (FIPS PUB 1-2) incorporates the American Standard Code for Information Interchange (ASCII) which specifies a set of characters for interchanging information between computers. Federal Information Processing Standards Publication 1-2 (FIPS PUB 1-2) defines several proper subsets of this set to be used for special applications. The 95-

character graphics subset specified in FIPS PUB 1-2 is the set from which the System Manager and Security Officer should select the acceptable composition for a particular system. While backspaces can be used effectively to mask printed passwords, several comments on the draft guidelines described the special use of backspace in many computer systems and recommended that it not be allowed.

The minimum composition contains 10 characters because some systems (e.g., financial transaction systems) use a 10-digit PIN PAD (Personal Identification Number entry device) for entering the password which is called a PIN. The PIN PAD looks very similar to the keyboard of a push button telephone. Some systems being developed use the push button telephone for data entry and retrieval. Users of these systems stated their desire to use the Standard. A better composition contains 16 characters which includes the 10 digits plus (A,B,C,D,E,F). This set can represent hexadecimal characters, each of which is a four-bit (binary digit) code. For example, 16 hexadecimal characters are used to represent a Data Encryption Standard key (see FIPS PUB 46) which can be used as a personal key in a cryptographic system. Many passwords are composed only of the 26 lower case letters (a-z) or the 26 upper case letters (A-Z). However, using either of these sets often encourages the selection of a person's initials, name, nickname, relative, hometown, or common word easily associated with the person. Even allowing all possible 4-letter, 5-letter or 6-letter English words greatly restricts the number of passwords when compared to all possible passwords of length range 4-6 with the same composition. Totally alphabetic password composition should be discouraged. The best password composition is the 95-character graphic set as specified in FIPS PUB 1-2 (see app. C).

3.2 Length

Length is closely associated with composition in assessing the potential security of a password system against an intruder willing to try exhaustively all possible passwords. The length of a password provides bounds on the potential security of a system. A length of exactly 1 reduces the potential number of valid passwords to the number of characters in the acceptable composition set. A length of 2 squares this number; a length of 3 cubes this number; a composition of 10 and a length of exactly 4 provides for 10- (read 10 raised to the fourth power) or 10,000 possible passwords. PINs are typically four digits because of low security requirements, for ease of remembering by a large customer base and for speed and accuracy of entry. A PIN verification system generally prevents a person from quickly trying all 10,000 possible PIN's for a particular valid financial account in order to find the valid PIN. If the trial and error process can be automated, even on a small home computer, the valid PIN can be found in a few minutes. Having a length range of 4-6 increases the possible number of PIN's to 1,110,000 ($10^6+10^5+10^4$).

If all other factors are temporarily ignored, the security provided by a password is directly proportional to the allowed length of the password. In other words, longer passwords are more secure. However, other factors cannot be ignored in practical password systems. Long passwords take longer to enter, have more chance of error when being entered, and are generally more difficult to remember (the latter may not be true unless the password consists of random characters). Sixteen random hexadecimal characters are very difficult to remember and are very difficult to enter quickly and accurately. For this reason, DES keys are usually not personal passwords and vice versa. However, long passphrases can be transformed to virtual passwords of exactly 64 bits (or 56 bits with the other 8 bits recomputed to be parity bits). Long passphrases can be easy to remember but still take longer to enter.

The length range should include a number of lengths, probably from 5-8 characters, and the composition should be a large set so that a high level of security can be provided easily.

A passphrase is an understandable sequence of words (sentence, sentence segment, phrase) that can be transformed and stored as 64 bits, and which is used as a password. A passphrase is generally easy to remember by the owner of the passphrase, and hence is allowed on some systems because of this characteristic. Since the number of distinct possibilities of understandable passphrases is considerably smaller than for a random sequence of characters of the same length, a longer passphrase is preferable to a shorter one. For example, the number of understandable 64-character long passphrases composed using the 27-character set A-Z and space, is considerably less than 27^{64}, which is the number of possibilities if the characters are selected randomly.

A passphrase may be used that is equivalent to a password as specified in the Standard. A passphrase may be transformed into a virtual password by using a transformation such as a hashing function or a cryptographic function. These functions should compute a value using the entire passphrase as input such that any change in the passphrase should result in a different computed value (within some probability). The value that is computed is the virtual password and must be 64 bits as specified in the Standard. This allows all password systems to allocate a maximum of 64 bits for storing each password, and therefore allows up to 2^{64} possible passwords (many thousands of years of security against exhaustive searching attacks). Such a passphrase thus provides the benefits of being easily remembered at the added cost of additional time to enter the longer passphrase and the time needed to compute the virtual password. The Data Encryption Standard (FIPS PUB 46) and the cipher block chaining mode specified in the DES Modes of Operation Standard (FIPS PUB 81) are suggested as the transformation (see app. D).

3.3 Lifetime

The security provided by a password depends on its composition, its length, and its protection from disclosure and substitution. The risk associated with an undetected compromise of a password can be minimized by frequent change. If a password has been compromised in some way and if a new password is created that is totally independent of the old password, then the continued risk associated with the old password is reduced to zero. Passwords thus should be changed on a periodic basis and must be changed whenever their compromise is suspected or confirmed.

The useful lifetime of a password depends on several variables, including:

- The cost of replacing a password;

- The risk associated with compromise;

- The risk associated with distribution;

- The probability of "guessing" a password;

- The number of times the password has been used;

- The work of finding a password using exhaustive trial and error methods.

Password systems should have the capability of replacing the password quickly, initiated either by the user or the Security Officer. Passwords should be changed voluntarily by the owner whenever compromise is suspected and should be changed periodically with a maximum interval selected by the Security Officer. The interval may be a period of time or depend on a number of uses. The password system itself should have automated features which enforce the change schedule and all the security criteria for the installation. The system should check that the new password is not the same as the previous password. Very sensitive applications may require that a new password not be the same as any of the previous two, three, ..., N passwords. Such

a system requires storage for N passwords for each user. It should not be a requirement of a system that the password for each user be unique. Having a new password rejected for this reason confirms that another user has the password.

3.4 Source

Passwords should be selected at random from the acceptable set of passwords by either the owner or the password generator. However, this guidance may not be possible in all cases and may not be desirable in some cases. The Security Officer often selects a password for a new user of a system. This can be used for the first access to the system. The system may then require that the user replace this password which the Security Officer may know with a password that only the user knows. Passwords that are created or selected by a user should be checked by the automated password system as meeting all of the criteria of the password system. Passwords that do not meet all the criteria should b(' rejected by the automated password system. A record that an attempt to select an unacceptable password may be made by some automated systems but is not required by the Standard.

If passwords are generated by the system, the method of generation should not be predictable. Commonly used random number generators that are available. in computer systems for statistical purposes should be avoided because the sequence of random numbers that they generate are predictable. The DES algorithm, together with a non-deterministic parameter such as the least significant bits of a high resolution computer system clock may be used. The results of a random generator are then combined with password selection rules to obtain a password which meets mandatory and desirable criteria.

3.5 Ownership

A personal password should be individually owned rather than owned in common by a group of individuals in order to provide individual accountability within a computer system. This is desirable even though a group of people all have common access privileges to the same resources or data. Individual ownership of personal passwords is required because:

- It can establish individual accountability for the determination of who accessed what resources and for what purposes.

- It can establish illicit use of a password or loss of a password.

- It can be used for an audit trail of the activities of a user.

- It avoids the need to change the password of an entire group when a single member of the group leaves or loses authorization privileges.

3.6 Distribution

A password must be transported from the owner to the authentication system if selected by a user, from the authentication system to the owner if generated by the password system or from the Security Officer to both the owner and the authentication system if generated by the Security Officer. The initial password is often distributed in a different manner than subsequent replacement passwords. The initial password is generally created and issued directly, either orally or in writing, Curing the meeting at which a user is initially authorized use of the computer system or access to a set of data. This may be a one-time password which must be changed after the initial access request is granted. Changing of a password by a user generally requires that the user supply the old password and then the replacement password. The replacement is checked for meeting the security requirements of the system, checked that it is different than the old password, and then entered into the storage location of the old password. An audit record should be made of the replacement, containing the date and time of the change, but not the new password Forgotten passwords should be replaced and a new password issued in a manner similar to, if not identical with, issuance of the initial password.

Passwords that are distributed in writing should be contained in a sealed envelope marked "To be opened by addressee only." Delivery may be by courier, internal 'nail, or by U.S. Mail. Instructions to the user should be to:

-Destroy the written password after memorizing it; or

-Return the written password to the Security Officer after signing the receipt for the password and after sealing it in the return mailer.

-Use the password as soon as possible and, if the password can be changed by the user, change the password.

Some systems distribute passwords in a sealed mailer that has been printed by a computer. The mailer is designed so that it cannot be resealed once it is open. The password is printed only on the inside of the mailer on the second page using carbon paper attached to the back of the mailer's front page. The instructions say to remove the front of the mailer, which shows the name of, 'the intended recipient, to destroy the front and save the password (in a protected place readily accessible only to the intended recipient). The part of the mailer that has the password has no other identification which would associate the password with either the system or the owner. Thus, anyone finding a lost password would usually not be able to use it. While not as desirable as memorizing the password and destroying the distribution medium, this system is useful when passwords are not routinely used and would be written in a location which-is more easily associated with the owner.

When distributed by a secure mailer, a receipt for the password may be validated by positive response or on an exception basis. When password distribution is done on an unscheduled basis, a positive response,is required. When passwords are distributed regularly, the user should be expecting a new password and should report any failure to obtain a new password.

In either case, a record must be kept of the fact that a new password was issued.

There may be a transition period in which it is uncertain if the old password is valid or if the new password is valid. Some systems may allow either password to be valid during the transition period. This means that both passwords must be stored and compared with an entered password. Some systems may have no transition period (e.g., a password becomes valid at 8:06 P.M. exactly) and record attempts at using the old password in an audit file. A report of such attempts should be sent securely to the password owner as notification that usage of an old password was attempted. The owner can verify that the use was an accidental rather than an unauthorized use of an old password by an intruder.

3.7 Storage

Passwords should be stored in the authentication system in a manner which minimizes their exposure to disclosure or unauthorized replacement. Several methods have been used to protect passwords in storage. Most systems have a password file that can be legitimately read only by the "LOGON" program. The file is protected by a file access mechanism which checks a protection bit in a file access table. Only the privileged LOGON program has access to read the file and only (:he password program has access to write the file. 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. Some systems encrypt the passwords, either reversibly (two-way) or irreversibly (one-way) using a Data Ecrypting Key (DEK) or the password itself as a key. Of course, any key (e.g., a Data Encrypting Key) retained in storage would also need protection by encryption using a Key Encrypting Key (KEK). The type of 'protection provided to the passwords should be commensurate with the protection desired for the system or data and hence a protection system should be used to provide the desired protection.

One-way encryption of passwords is allowed in the Standard when encryption is used for stored password protection. One-way encryption systems transform the password in such a way that the original password can not be recovered. This protects the original password from everyone, including the Security Officer and the systems programmers. When a user is logging onto such a system, the password that is entered by the user is one-way encrypted and compared in encrypted form with the stored encrypted password. The same encryption method and key must be used to encrypt the valid password before storage and to encrypt the entered password before comparison.

Two-way encryption of passwords is also allowed in the Standard. Given the correct key, the original password may be determined from the encrypted password. A user entered password may be compared with the decrypted stored password (which was encrypted), or the user's password may be encrypted and compared with the stored password as is done with one way encrypted passwords.

3.8 Entry

Entry of a password into an automated authentication system in a secure manner is often a difficult task. An observer often is able to detect part or all of a password while the user is entering the password. Typing keyboards are the typical entry device. A user that is not a trained typist often enters the password with one finger. A long, random password that is difficult to enter may be more vulnerable to observation than a short easily entered password. The Standard specifies that a password shall be entered by a user in such a manner that the password will not be revealed to anyone observing the entry process. The following discussion provides some techniques which the user may find useful in achieving this goal and which the computer systems operation staff may find useful in assisting the user.

The computer terminal, keyboard, push-buttons, or password entry device should provide a means for minimizing the exposure of the password during entry. The password should not be printed on the terminal during the entry process. If the keyboard and the terminal display or printer are directly coupled, then the password should be masked by obliterating (understriking) the space where the password is going to be printed. The password may be masked further by overstriking the area after password entry. Computer generated masks used during password entry to disguise the entered password should not always be the same. In any case no printed or displayed copy of the password should exist after password entry.

CRT terminals which use half-duplex communications may present a problem because the password overwrites the understriking and remains visible on the display. The display should be immediately cleared by the password entry program after password entry in such systems. Users should be instructed to manually clear the display following password entry if the screen cannot be cleared by the password entry program.

When submitted as a part of a remote entry batch processing request, the password should be added to the request at the last possible moment and physically protected. Batch processing requests submitted in punched cards should have the password card added by the user just prior to submission. The computer operations staff should maintain the card decks in a protected area and should remove and destroy the password card after the deck has been read by the system. The password should never be printed on any output media. One-time passwords that are distributed to the owner in the form of a password list and sequentially used for sequential batch processing requests may be used. The Standard requires that such lists be physically protected by the owner.

Users should be allowed more than one attempt to enter a password correctly in order to allow for inadvertent errors. However, there should be a maximum number of trials allowed for a password to be entered correctly. A maximum of three (3) attempts is considered adequate for typical users of a computer system. The system should also prevent rapid retries when a password is entered incorrectly. Several seconds should elapse before another password is requested. This prevents an automated, high speed, trial-and-error attack on the password system. A security record should be maintained of the fact that incorrect passwords were entered but the incorrect password should not be kept in the record. A security alarm should be generated if:

1. The maximum number of allowed password retries is exceeded;

2. The maximum number of allowed failed logons from one terminal is exceeded;

3. The maximum number of allowed failed logons for a time period is exceeded.

These parameters must be set according to the sensitivity of the data being protected, the profile of the typical system user and the policy of the organization. Some organizations will be willing to set the parameters high to prevent customer dissatisfaction while other organizations will set the parameters low to prevent security compromises. Terminals should be disabled and users should be denied service if these parameters are exceeded. The Security Officer should be the only one who can enable the terminal and restore the service of the user following these events.

The system should inform the user, following a successful LOGON procedure, of the last successful access by the user and of any unsuccessful intervening access attempts. This will aid in uncovering any unauthorized accesses or attempted accesses which may have occurred between successful accesses. The user can do several actions to prevent an observer from learning the password by watching the password entry process. First, entry of the password can be practiced so that it can be quickly entered using several fingers. Second, the body can be used to prevent the observer from seeing the keys being pressed during password entry. Third, the user can request that a guest not watch the password entry process. Fourth, the user can perform the password entry prior to demonstrating use of the system.

3.9 Transmission

Passwords are typically used to authenticate the identity of a user attempting to gain access to a shared computer system or network from a terminal. In order to be authenticated, the password is typically transmitted from the terminal to the computer via the communication line between the terminal and the computer. Unless the communication line is physically protected or encrypted, the password is vulnerable to disclosure. Most communication lines between terminals and computers are not afforded this protection at present. Therefore, users should be aware that their passwords can very easily be disclosed via passive wiretapping.

Computer systems can also be easily spoofed. This can occur if an intruder has inserted an active wiretap between a terminal and the computer. An active wiretap can be built today for several hundred dollars by a home computer hobbiest. The wiretap can be built into a briefcase and consists of a hobby computer with a receive/transmit communication chip which receives data from the terminal and computer and then retransmits data to the computer and terminal, having scanned and modified the data. The active wiretap can replace one user's password with another user's password, even if the passwords are encrypted at the terminal. Spoofing occurs when the system is fooled into "believing" one user is at the terminal when another user is actually there. Reverse spoofing occurs when a user is fooled into believing that communication is with the intended computer when another computer is there. In the latter case, an authorized user can be spoofed into providing the valid user's password by simulating the "LOGON" request of the intended computer. After the password is obtained, the intruder that is controlling the spoofing computer informs the user that the requested service is temporarily unavailable. During this exchange the intruder has obtained a valid password without the user's knowledge.

These threats can be prevented by one of two encryption methods. First, the communication line between the terminal and the computer can be protected by encryption devices which use a secret key (e.g., a Data Encrypting Key) for encrypting all communication between the terminal and the computer. Transmitted passwords are thus protected from disclosure. In addition each transmission can be numbered so that a previous transmission cannot replace a later transmission (.i.e., a previously used valid password cannot be saved and used to replace an invalid password, even if both are encrypted). Passwords are thus protected to the same degree as the data as specified in the Standard.

Alternatively, the password can be used as the encryption key or as part of the encryption key. Suppose a user enters a password to be used as an encryption key at the terminal (i.e., never transmitted to the computer) and the user's password is retrieved from the computer's memory and used as the encryption key at the computer (i.e., never transmitted to the terminal). Then the terminal and the computer are mutually authenticated if normal communication can occur using the encryption and decryption processes at the terminal and computer, both using the password as the key (or a part of the key). This alternative is also allowed in the Standard.

In order to prevent compromise of the level of security provided by the cryptographic mechanism, the Standard specifies that personal passwords that are used as keys as described above be selected at random from the set of all possible encryption keys used by the cryptographic process. It also specifies that passwords that are used as Data Encrypting Keys should not also be used as Key Encrypting Keys, and vice versa. This is to minimize any possibility of attempting to recover the key (and hence the password) through cryptanalytic techniques.

3.10 Authentication Period

Interactive "sessions" between a user and a computer via a remote terminal often last several hours. While security policy should state that a terminal that is "logged onto" a computer should never be left unattended

by the user that is "logged onto" the computer, in practice this often occurs. Many systems have a feature which automatically logs a user off the system if the terminal has been inactive for some period of time. This is to prevent someone who encounters an unattended terminal from using it. Some access control systems require that a user be reauthenticated on a periodic basis in addition to the initial authentication process. These systems often antagonize the user if the authentication frequency is set too high. The message that the authentication process must be performed again often comes in the middle of the work that a user is performing. If this work happens to be a large printout of final text of a paper to be published, the user is rightfully upset. For this reason the Standard did not specify a minimum reauthentication period. Reauthentication should only be required to satisfy high security requirements, and then only requested if the terminal has been inactive for a period of time. This should prevent the authentication process from occurring in the middle of some important work.

4. Examples of Password Systems

The following examples of password systems which satisfy various security requirements are provided as assistance to Security Officers and System Managers. Determination of the parameters for each of the 10 factors discussed above will permit the preparation of the Password Standard Compliance Document. These examples should not be considered as the only selection of the parameters for the 10 password system factors.

4.1 Password System for Low Protection Requirements

A hypothetical password system might have the following parameters for the 10 factors which will both satisfy the Standard and satisfy requirements for protection which are considered to be minimal. The example is similar to that found in many retail, customer initiated financial transaction systems in which the maximum liability of the customer is $50 and the maximum liability of the bank is limited by the number of transactions allowed per day. This example is also typical of many government-owned, government-leased computer systems in which no sensitive applications are performed. Small scientific systems, special purpose systems and systems not making critical automated decisions may fall in this category. Systems which have limited financial liability and those which require only accountability and control of computer usage and costs may also be considered in this category.

1. Length Range: 4-6
2. Composition: Digits (0-9)
3. Lifetime: 1 year
4. Source: User
5. Ownership: Individual (personal password); group (access passwords)
6. Distribution: Unmarked envelope in U.S. Mail
7. Storage: Central computer on-line storage as plaintext
8. Entry: Non-printing "PIN-PAD"
9. Transmission: Plaintext
10. Authentication Period: Each transaction

4.2 Password System for Medium Protection Requirements

Government systems which process limited "sensitive" applications may fall in this category. These are applications which process data leading to or directly related to monetary payments or process data subject to the Privacy Act of 1974. Agency management may determine that additional applications should be designated as sensitive. Computer systems that are subject to fraud, theft, erroneous payments or other loss of sensitive information may also fall into this category. Government systems which make payments (e.g., Social Security, Treasury), keep inventories (e.g., Armed Forces), and process personal information (e.g., Internal Revenue

Service, Department of Education) would be examples of systems which would have requirements of this nature and probably would be satisfied by this type of password system.

1. Length Range: 4-8
2. Composition: U.C. Letters (A-Z), L.C. Letters (a-z), and digits (0-9)
3. Lifetime: 6 months
4. Source: System generated and user selected
5. Ownership: Individual
6. Distribution: Terminal and special mailer
7. Storage: Encrypted passwords
8. Entry: Non-printing keyboard and masked-printing keyboard
9. Transmission: Cleartext
10. Authentication Period: Login and after 10 minutes of terminal inactivity.

4.3

Password System for High Protection Requirements

Computer systems which process information of a sensitive nature and which rely on passwords to provide personal identification may have high protection requirements that could be satisfied by a password system for personal identification having these characteristics.

Systems having high protection requirement's may include those which have unusually high potential for fraud or theft, have a high economic benefit to a system intruder, and have a substantial impact on safety or the well being of the society. Some computer systems of the Department of Defense or the Federal

Reserve Communication System may fall into this category. Systems having very high security requirements may require methods of personal identification which are based on physical characteristics of a person (signature, voice, fingerprint) or on a combination of something unique that the person has (e.g., badge, ID card) and something unique that the person knows (i.e., a password). A risk analysis should be performed for each government owned or leased computer system to determine its security requirements and then a personal identification system should be selected which best satisfies these requirements.

1. Length Range: 6-8
2. Composition: Full 95 character set
3. Lifetime: One month
4. Source: Automated password generator within the authentication system
5. Ownership: Individual
6. Distribution: Registered mall, receipt required; personal delivery, affidavit required
7. Storage: Encrypted passwords
8. Entry: Non-printing keyboards
9. Transmission: Encrypted communication with message numbering
10. Authentication Period: Login and after 5 minutes of terminal inactivity.

APPENDIX B

EXAMPLES OF COMPLIANCE AND PROCUREMENT DOCUMENTS

1.

Example of a Minimum Security Compliance Document

ORGANIZATION
:

XYZ Agency

TYPE OF
SYSTEM
:

Inventory

PREPARING
OFFICIAL
:

Samual V. Jones
DATE: 14 February 1986

JUSTIFICATION:
Analysis of the security requirements for the inventory system to be used by this agency indicates the desirability of implementing a password authentication system. It was further determined that a minimum compliance with the Federal Information Processing Password Usage Standard would fulfill the security needs of this system. Accordingly, the following criteria have been selected for the 10 basic factors specified in the Standard.

1. Length Range: 4-6
Rationale
: A minimum level of security for the data is required.

2. Composition: Digits (0-9)
Rationale
: Personnel are accustomed to PINs for their financial transactions and to combination locks. A numeric keypad is used.

3.
Lifetime
: One year
Rationale
: The maximum password lifetime is more than adequate for this system.

4. Source: User
Rationale
: Users desire to select passwords which are easy to remember, but will be instructed to select random passwords rather than those having particular significance to them.

5. Ownership: Individual (personal passwords); group (access passwords)
Rationale
: The Standard requires individual ownership of personal passwords. The group password is used for access control for this minimum level security system.

6. Distribution: Initial password given to any current authorized user to enter; subsequent passwords from a terminal following access authorization
Rationale
: All personnel authorized to use the system can receive passwords from the Security Officer.

7. Storage: Central computer on-line storage as plaintext
Rationale
: Data is not highly sensitive.
8. Entry: Non-printing keypads
Rationale

: Inexpensive and available.

9. Transmission: Plaintext
Rationale
: All data is contained in one building.

10. Authentication Period: Login
Rationale
: Minimum security requirements.

2.

Example of a Procurement Specification for a Minimum Security Password System

The operating system shall include a password system which includes the following features as a minimum.

(a) A password length range of 4-6 characters; characters to be selected from the digits 0-9.
(b) Passwords are to be selected by the users. Individual authorized users must have the capability of entering new users onto the system and deleting current users from the system. All interactions with the password system will be via video terminals.
(c) Passwords stored in the system may be stone as plaintext.
(d) User authentication shall be performed during the login process.

3.

Example of a Medium Security Compliance Document

ORGANIZATION
:

Department of Secrecy
TYPE OF
SYSTEM
:

Personnel Records
PREPARING
OFFICIAL
:

Constance Johns

DATE

:

7 July 1985

JUSTIFICATION:

The computer system containing the Department's personnel records currently uses passwords to authenticate an individual's identity for access to the system. A security analysis has determined that a level of protection greater than the minimum level of protection specified in the Federal Information Processing Password Usage Standard is required for this system. The following criteria have been selected as adequate to meet our requirements, and are hereby submitted for approval.

1. Length Range: 48
   Rationale:This allows a wide range of passwords from which to select.

2. Composition: (A-Z), (a-z) and (0-9)
   Rationale
   : Ease of password creation and remembering.
   Together with the length, this allows for selection of $62^8+62^7+62^6+62^5+62^4$ possible passwords if characters are selected randomly.

3.
Lifetime
: 6 months

   Rationale
   : Analyzed sensitivity of the data.

4. Source: Automatic password generator within the system. The user may refuse generated pass-words and request that another
   be generated.
   Rational
   : To eliminate the possibility that users will select passwords significant to them and easily guessed by others.

5. Ownership: Individual
   Rationale
   : Bach person is to be individually authenticated.

6. Distribution: Initial password from Security Officer access mailer; subsequent passwords from a terminal following access authorization
   Rationale:All entry and retrieval is performed using video terminals.

7. Storage: Encrypted passwords with access only by the password system
   Rationale:Sensitivity of the data. Passwords are used as the

encryption keys to encrypt the identifiers, and the result is stored at the central system.

8. Entry: Video terminals, non-printing
   Rationale: All entry and retrieval operations are performed at these terminals. Passwords are not displayed on the terminal during entry.

9. Transmission: Cleartext communications
   Rationale: While personnel data is sensitive, it is not necessary to encrypt the data during communication within the facility.

10. Authentication Period: Login and after 10 minutes of terminal inactivity.
    Rationale: Wish to avoid having carelessly vacated terminals used by unauthorized individuals.

4. Example of a Procurement Specification of a Medium Security Password System

The operating system shall contain a password system which will authenticate the identity of authorized users whose personal passwords are stored in the system. The password system shall consist of the following features at a minimum.

(a) Passwords shall be composed of the characters A-Z, a-z, and 0-9. The system shall verify that only these legal characters are used in passwords.

(b) The length of a password shall be from 4 to 8 characters. The system shall not allow passwords to be selected outside this range, and shall requery for a valid entry.

(c) The system shall maintain a record of the date of password creation and last password modification, and shall enforce a password update at a time interval entered during SYSGEN.

(d) Passwords shall be generated by an automatic password generation program in the system whose algorithm has been approved by this Agency. Users shall have the capability of refusing any generated password and requesting another to be generated. The system shall not allow further system activity by a user until a new password has been selected.

(e) The initial password for a user shall be entered by a Security Officer after entering a special Security Officer password. Thereafter, passwords are to be changed by users after successful access authorization. A record shall be maintained of the date and time of password assignment/modification along with the identity of the individual with whom the password is associated. However, no record shall exist of the plaintext password selected.

(f) Passwords are to be stored in encrypted form, and this information shall only be accessible by the password system. Personal passwords shall be stored along with the identifier of the user owning the password. These passwords shall be encrypted by using the plaintext password as a key to encrypt the identifier using DES in the ECB mode.

(g) Entry of passwords shall be performed using video terminals. Entered passwords shall not be visible on the terminal. A maximum of three entry attempts shall be allowed. A time delay of at least 15 seconds shall be enforced before another set of three entry attempts may be made. A record shall be made of unsuccessful entry attempts. After three sets of unsuccessful attempts within a 5-minute interval, a message shall be displayed on the system operator's console and a bell shall be continuously sounded until the message is acknowledged.

(h) Transmissions to remote terminals shall be cleartext. Messages to remote terminals shall include message sequence numbers.

(i) User authentication shall be requested during login and after 10 minutes of terminal inactivity. Service shall be denied when the correct passwords are not entered.

APPENDIX D

PASSWORD ENCRYPTION AND PASSPHRASE TRANSFORMATION

The FORTRAN program provided herein is a suggested method for password encryption and passphrase transformation. The program transforms a user identifier (USER-ID) and a user password (4-8 characters) or passphrase (9-64 characters) into 64-bit values for subsequent encryption. This capability was suggested by several people in comments to NBS on the Password Usage Standard. Limited experience has indicated that passphrases (greater than eight characters) are easier to remember and enter than passwords consisting of any combination of eight characters from the 95 character set suggested in the Standard. The method provided in this appendix is cryptographic algorithm independent, although 64-bit vectors are used. Key consists of 56 significant bits plus eight bits of parity. Input and output are each 64 bits in length.

The program allows the entry of passwords consisting of all characters from the 95 character set. Acceptable entries include passwords (4–8 characters), passphrases (9–64 characters), the equivalent eight character virtual password, or the equivalent 16 hexadecimal digit pass key. The last two are printed whenever a passphrase is entered. User IDs up to 64 characters long may also be entered. However, the transformed virtual value for the user ID is not (normally) printed. User IDs and passwords which are entered and are not a multiple of eight characters in length are padded with spaces.

A virtual password or user ID is calculated whenever a value greater than 8 characters in length is entered and (for passwords only) which does not consist of precisely 16 hexadecimal characters. The virtual value is produced by CBC encryption using the first eight bytes as key, and subsequent 8-byte blocks as input to the CBC algorithm. The virtual value is selected in 7-bit groups from the final output of this operation. These 7 bits are stored in the right-most bits of a byte, and the left-most bit is set to zero. Seven bit values which are not represented in the 95-character set result in discarding the left-most bit and adding the next bit from the final output value of the encryption operation. If all bits from this final output value are used before a complete 8-byte virtual password or user ID has been calculated, the output value is again processed by the encryption

operation to produce an additional 64 bits from which to complete the virtual password or user ID calculation. The value which is ultimately stored as the encrypted password is produced by encrypting the user ID (or virtual user ID) by a key which is the exclusive OR of the password (or virtual password) and a system key. The system key may be set to 0 for system independent operation (i.e., for intercommunication between systems).


```
C    PASSWORD ENCRYPTION AND PASSPHASE TRANSFORMATION DEMONSTRATION PROGRAM.
     FC   VERSION 1.2
C    THIS PROGRAM WAS PRODUCED BY THE COMPUTER INTEGRITY AND SECURITY STAFF,
C    INSTITUTE FOR COMPUTER SCIENCES AND TECHNOLOGY
C    TECHNOLOGY A-216
C    NATIONAL BUREAU OF STANDARDS
C    GAITHERSBURG, MARYLAND 20899
C    (301)921-3427
C
C
C    THE PROGRAM 15 DESIGNED TO COMBINE A USER'S
C    IDENTIFIER WITH THE ASSOCIATED PASSWORD 50 THAT THE RESULT CAN NEVER BE
C    DIVIDED OR DECIPHERED.  THE RESULT IS AN ENCRYPTED PASSWORD
C    WHICH CAN BE COMPARED WITH A PREVIOUSLY ENCRYPTED AND
C    STORED PASSWORD.  THE DESIGN GOALS INCLUDE HAVING A SYSTEM FOR
C    ENCRYPTING PASSWORDS THAT DOES NOT USE A STORED CRYPTOGRAPHIC KEY.
```

```
C     SUCH SYSTEMS CAN EASILY PASS AN ENCRYPTED PASSWORD TO ANOTHER COMPUTER
C     SYSTEM FOR VALIDATION.  FOR SYSTEMS THAT DO NOT WISH TO USE ANOTHER
C     COMPUTER TO VALIDATE PASSWORDS OR TO INTERCHANGE PASSWORDS, A SYSTEM
C     KEY VARIABLE IS PROVIDED WHICH SHOULD BE RANDOMLY SET FOR EACH SYSTEM.
C     THE SYSTEM KEY SHOULD BE SET TO ZERO FOR INTERCHANGE AND A SECRET VALUE
C     FOR NO INTERCHANGE.  IDENTICAL TRANSFORMATIONS ARE USED FOR THE
C     USER-ID AND PASSPHRASE.
C
C
C     THE USER-ID AND THE PASSPHRASE CAN EACH CONTAIN UP TO 64 CHARACTERS.
C     PASSPHASES AND LONG USER-IDS (MORE THAN 8 CHARACTERS EACH)
C     ARE TRANSFORMED TO 64 BIT VALUES.  THE RESULTS, CALLED THE VIRTUAL
C     USER-ID AND VIRTUAL PASSWORD, ARE THEN USED TO PRODUCE AN ENCRYPTED
C     PASSWORD USING A ONE-WAY ENCRYPTION FUNCTION.
C
C     A USER-ID AND A PASSPHRASE (PASSWORD/PASS KEY) ARE ENTERED BY A
C     PERSON DESIRING USE OF A SYSTEM.  THE USER-ID AND PASSPHRASE ARE
C     TRANSFORMED. THE VIRTUAL PASSWORD IS USED AS A KEY TO ENCRYPT
C     THE VIRTUAL USER-ID AND THE RESULT IS COMPARED WITH THE STORED
C     VALUE FOR THE AUTHORIZED USER OF THE SYSTEM.
C
C     BOTH THE PASSWORD ENCRYPTION AND PASSPHASE TRANSFORMATION OPERATIONS
C     USE THE DATA ENCRYPTION STANDARD (DES) ALGORITHM, BUT ANY BLOCK
C     ENCIPHERING ALGORITHM CAN BE USED.
C
C     CALLS TRANSF, PARITY, CBC, HEXKEY, PACK, UNPBIN, DES AND SETKEY ROUTINES
C     DESCNT IS THE NUMBER OF TIMES TO ENCRYPT PASSWORD (ODD *).
      INTEGER DESCNT/5/
      INTEGER USERID(64) , PASSWD(64) . SYSKEY(8)
      INTEGER SPACE /' '/,IDLEN, PWLEN , HEXFLG
      INTEGER IDBIN(64) ,KEYBIN(64) , SYSBIN(64)
C     THE SYSTEM KEY SHOULD BE ALL ZEROS FOR INTERCHANGE WITH OTHER SYSTEMS.
C     FOR SYSTEMS THAT WILL NOT INTERCHANGE PASSWORDS WITH OTHER SYSTEMS,
C     THE SYSTEM KEY SHOULD BE SET TO RANDOM EVEN NUMBERS BETWEEN O AND 254
C     DECIMAL (INCLUSIVE) IN EACH OF THE EIGHT ENTRIES.  THIS IS THE EQUIVALENT
C     OF A DES KEY WITH THE RIGHT-MOST BIT OF EACH OCTET RESERVED FOR PARITY.
C     **NOTE:  THE FOLLOWING SHOULD BE CHANGED FOR EACH SYSTEM INSTALLATION.**
      DATA SYSKEY/120,98,46,76,22,2,254,128/
C     INITIALIZE USER-ID AND PASSPHRASE VECTORS
1     DO 4 1=1,64
      USERID( I) =0
4     PASSWD(I)-O

C     GET USER ID AND PASSPHRASE AND DETERMINE THEIR LENGTHS
5     WRITE(6,800)
800   FORMAT(//' ENTER USER ID: ')
      READ(S, 100) USERID
      CALL TSTVAL( 64 , USERID, IDLEN)
      IF(IDLEN.LE.0) STOP
```

```
C      FOLLOWING STATEMENT IS PROGRAM DEBUG STATEMENT
C      WRITE(6,500) (USERID(M),M=1,IDLEN)
500    FORMAT(' ASCII= ',8Z2.2)
10     WRITE(6,900)
900    FORMAT(' ENTER PASSWORD, PASSPHRASE OR 16-DIGIT HEX KEY ')
100    FORMAT(64A1)
       HEXFLG=0
       READ(s, 100)PASSWD
       CALL TSTVAL( 64, PASSWD, PWLEN)
       IF (PWLEN.LT.4) GO TO 10
C      CHECK FOR A PASSWORD ENTERED AS A HEXADECIMAL KEY IF (PWLEN. EQ. 16) CALL HEXKEY(PWLEN,
       PASSWD,HEXFLG)
C      PASSWORD MUST BE DIFFERENT THAN USER-ID; CHECK AND REPORT.
       IF (IDLEN.NE.PWLEN) GO TO 23 DO 22 I=1,IDLEN
                                IF (PASSWD(I).NE.USERID(I)) GO TO 23
22               CONTINUE
                 WRITE(6,200)
200              FORMAT(' PASSWORD MUST NOT EQUAL THE USER ID')
                 GO TO 10
23     CONTINUE
C      FOLLOWING STATEMENT IS FOR PROGRAM DEBUG. WRITE(6.500) (PASSWD(M),M=1,PWLEN)
C      TRANSFORM LONG USER-ID INTO VIRTUAL USER-ID IF REQUIRED.
       IF (IDLEN .LE. 8) GO TO 43 CALL TRANSF( IDLEN , USERID)
C                FOLLOWING STATEMENT IS FOR PROGRAM DEBUG.
C                WRITE(6,650)(USERID(I),I=1,8)
650              FORMAT(' VIRTUAL USER ID IN 95 CHARACTER SET IS ',8A1)
43     CONTINUE
C      HEXFLG IS A 1 IF SIXTEEN HEX CHARACTERS WERE ENTERED.
C      SIXTEEN HEX CHARACTERS ARE USED AS A KEY, NOT A PASSPHRASE IF (HEXFLG .EQ. 1) GOTO 46
C      TRANSFORM PASSPHRASE INTO VIRTUAL PASSWORD IF MORE THAN
            8 CHARACTERS. IF (PWLEN .LE. 8) GO TO 44
                 CALL TRANSF(PWLEN, PASSWD)
                 WRITE(6,660) (PASSWD(I),I=1,8)
660              FORMAT(' VIRTUAL PASSWORD IN 95 CHARACTER SET IS ',8A1)
C                SHIFT EACH BYTE LEFT ONE BIT FOR DES PARITY BIT COMPUTATION
44          DO 45 1=1,8
                 PASSWD(I) = 2*PASSWD(I)
45          CONTINUE
                  IF (PWLEN .LE. 8)GO TO 46 WRITE(6,670) (PASSWD(I),I=1,8)
      670         FORMAT(' THE PASSWORD IN HEXADECIMAL IS ',8Z2.2)
      46    CONTINUE
      C     CALL SUBROUTINE TO UNPACK PASSWORD INTO BINARY VECTOR, ONE BIT PER WORD. CALL
            UNPBIN(8 ,8, PASSWD,KEYBIN)
      C     CALL SUBROUTINE TO UNPACK SYSTEM KEY MASK INTO BINARY VECTOR. CALL UNPBIN(8 ,8,
            SYSKEY, SYSBIN)
      C     EXCLUSIVE OR THE PASSWORD AND THE SYSTEM KEY TO MAKE AN ENCRYPTION KEY DO 24
            1=1,64
      24    KEYBIN(I)=MOD(KEYBIN(I)+SYSBIN(I),2)
      C     SET PARITY OF KEY CORRECTLY BEFORE USING
            CALL PARITY(KEYBIN)
      C     THE FOLLOWING TWO STATEMENTS MAY BE USED FOR PROGRAM DEBUG.
      C     CALL PACK(8,8,KEYBIN,PASSWD(9))
      C     WRITE(6,510) (PASSWD(M),M=9,16)
      510   FORMAT(' THE KEY FOR PASSWORD ENCRYPTION IS: ',8Z2.2)
      C     NOW LOAD THE KEY
            CALL SETKEY(KEYBIN)
      C     UNPACK THE USER ID OR VIRTUAL ID INTO IDBIN FOR ENCRYPTION CALL UNPBIN(8,8
            ,USERID, IDBIN)
      C     NOW CALL THE DES ROUTINE THE NUMBER OF TIMES SPECIFIED. DO 30 I=1,DESCNT
      C     THIS CALLS THE DES ROUTINE AND ONE-WAY ENCRYPTS IDBIN INTO IDBIN.
```