NOT MEASUREMENT SENSITIVE

MIL-HDBK-804 (OM)
15 FEBRUARY 1990

SUPERSEDING
NAVDAC PUB 17.10
MARCH 1984

MILITARY HANDBOOK

NETWORK USER ID AND PASSWORD PROCEDURES

AMSC N/A

AREA IPSC

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.

F O R E W O R D

1. This military handbook (MIL-HDBK) is approved for use by the Naval Data Automation Command (NAVDAC), Department of Navy (DON) and is available for use by all Departments and Agencies of the Department of Defense (DOD).

2. Beneficial comments (recommendations, additions, deletions) and any pertinent data which may be of use in improving this document should be addressed to: Commander, Naval Data Automation Command (COMNAVDAC), Washington Navy Yard, Washington, DC 20374-1662 using the Standardization Document Improvement Proposal (DD Form 1426) appearing at the end of this document or by letter.

3. The use of advanced communications network technology in the Navy makes review and refinement of current procedures for user IDs and passwords necessary. Also of importance is the clear definition of organizational roles and responsibilities for information systems (IS) security.

4. The Department of the Navy Computer Security Program has defined various roles and responsibilities for computer and network security in the Navy. The Worldwide Military Command and Control System (WWMCCS) has also identified responsibilities, procedures, and requirements for IS security throughout the WWMCCS community. The WWMCCS Intercomputer Network (WIN) accommodates roles and responsibilities that are similar, applicable, and adaptable to Navy network requirements. This handbook amplifies those roles and responsibilities as they apply to the administration and control of user identification (ID) and passwords Navy-wide.

5. This handbook was reviewed and considered by the Auditor General of the Navy for incorporation into the Naval Audit Service Automatic Data Processing Audit Program. This handbook was coordinated with the Defense Communications Agency for compatibility with Defense Data Network (DDN) and with the Joint Chiefs of Staff (JCS) for authorization to assign user IDs using Navy symbols defined in JCS Publication (PUB) 6-03.7 (supersedes JCS PUB 22). This handbook provides for changes in the user ID and related procedures, especially the standard user ID site code, since the initial publication of Naval Data Automation Command (NAVDAC) PUB 17.10 in March 1984.

C O N T E N T S

C O N T E N T S

1. SCOPE

1.1 Scope. This handbook describes the administrative procedures, common user ID format, and controls for user IDs and passwords within the Navy IS community for networked systems.

1.2 Purpose. The purpose of this handbook is to provide procedures for the administration and control of user IDs and passwords in the Navy network for networked systems support.

1.3 Content. This handbook is consistent with current Department of Defense (DOD) procedures for the WWMCCS and the DDN.

1.4 Applicability. The provisions of this handbook are applicable to users of Navy common user networks or networks which cross major Navy command boundaries (hereafter referred to as Navy networks), host computers, and terminals. Included are Navy networks classified below Secret, for example; Unclassified, For Official Use Only, Privacy, and Confidential.

2. APPLICABLE DOCUMENTS

2.1 Government documents.

2.1.1 Specifications, standards, and handbooks. The following specifications, standards, and handbooks form a part of this document to the extent specified herein. Unless otherwise specified, the issues of these documents are those listed in the issue of the DOD Index of Specifications and Standards (DODISS) and supplement thereto, cited in the solicitation (see 6.2).

FEDERAL INFORMATION PROCESSING STANDARDS (FIPS)

FIPS 112 - Password Usage (includes CSC-STD-002-85, see below). FIPS 112 is not listed in the DODISS of 1 November 1989.

(Copies of Federal Information Processing Standards (FIPS) listed in the DODISS are available to DOD activities from the Standardization Documents Order Desk, Building 4D, 700 Robbins Avenue, Philadelphia, PA 19111-5094. Others must order copies of FIPS from the National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161-2171.)

2.1.2 Other Government documents, drawings, and publications. The following other Government documents, drawings, and publications form a part of this document to the extent specified herein. Unless otherwise specified, the issues are those cited in the solicitation.

SECNAVINST 5239.2 of 15 Nov 1989	-	Department of the Navy Automated Information Systems (AIS) Security Program (Stock Number 0579-LD-054-7880) (cited in paragraphs 2.3 and 4.1.1).
OPNAVINST 5239.1A of 1 Apr 1985	-	Department of the Navy Automatic Data Processing Security Program with change 1 (Stock Number 0579-LD-051-1321) (cited in paragraphs 2.3, 4.1.1, 4.2.1, 4.2.2, and 4.3)
JCS PUB 6-03.7 of Apr 1988	-	Security Policy for the Worldwide Military Command and Control System (WWMCCS) Intercomputer Network (Stock Number 0579-LP-001-0750) (supersedes JCS PUB 22, WWMCCS ADP System Security Manual). JCS PUB 6-03.7 is cited in paragraph 5 on page ii and in paragraphs 4.1.2 and 4.3.1).
CSC-STD-002-85 of 12 April 1985	-	Department of Defense Password Management Guideline (included as appendix E of FIPS 112)

(Copies of SECNAVINST 5239.2, OPNAVINST 5239.1A and JCS PUB 6-03.7 are available from the Commanding Officer, Naval Publications and Forms Center, 5801 Tabor Avenue, Philadelphia, PA 19120-5099. Use DOD Single Line Item Requisition (DD Form 1348) citing the stock numbers shown above. Copies of CSC-STD-002-85 are available from the Superintendent of Documents (SupDoc), U. S. Government Printing Office (GPO), Washington, DC 20402, 202-783-3238, SupDoc stock number 008-000-00443-9, $1.75. Single copies are available to Government activities

without charge from the DOD Computer Security Center (CSC), Fort George G. Meade, Maryland 20755, Autovon 235-8742, Commercial 301-688-8742. However, CSC-STD-002-85 is reprinted as appendix E of FIPS 112.)

2.2 Non-Government publications. Not Applicable.

2.3 Order of precedence. Nothing in this handbook supersedes applicable laws and regulations unless a specific exemption has been obtained. In the event of a conflict between the text of this handbook and the Navy instructions cited herein, the Navy instructions take precedence. As stated in SECNAVINST 5239.2, that instruction takes precedence over OPNAVINST 5239.1A.

3. DEFINITIONS AND ABBREVIATIONS

3.1 Definitions. Definitions are contained in section 1 (Terms and Conventions) of FIPS 112 and in section 4 (Definitions) of appendix E of FIPS 112.

3.2 Abbreviations. Abbreviations with index to location by paragraph number or page and paragraph number for page ii (foreword) and appendix. Abbreviations which appear only in the appendix are not included.

ADPSO	Automatic Data Processing Security Officer, 4.2.1, 4.3.3, 4.3.5, 4.3.6, 4.4, 5.1.1, 5.2, 5.4, 5.5, 5.6, 5.7, 5.8. 5.9.1, 5.9.2
COMNAVDAC	Commander, Naval Data Automation Command, page ii, 2; 4.3.1; 4.2.1; 4.3.1; 5.1.1
CSC	Computer Security Center, 2.1.2; 5.6c
DD	Department of Defense, page ii, 2; 2.1.2; 6.3
DDN	Defense Data Network, page ii, 5; 1.3; appendix, 17.20
DOD	Department of Defense, page ii, 1; 1.3; 2.1.1; 4.1.2; 4.3.5; 5.1; 5.6c; 6.3
DODISS	DOD Index of Specifications and Center, 2.1.1; 6.2
DON	Department of the Navy, page ii, 2; 4.1.1
FIPS	Federal Information Processing Standard, 2.1.1; 3.1; 5.6
ID	Identification, page ii, 3,4,5; 1.1; 1.2; 4.1.2; 4.2.1; 4.2.2; 4.3.3; 5.1; 5.1.1; 5.1.2; 5.2; 5.3; 5.4b(1); 5.4b(2); 5.4b(3); 5.4c; 5.5; 5.6; 5.7; 5.8; 5.9.1; 6.1
IS	Information System, page ii, 3; 1.2; 4.1.1; 4.1.2; 4.2.1; 4.3.2; 4.4c; 5.4; 5.4b(2); 5.6; 6.1;
JCS	Joint Chiefs of Staff, page ii, 5; 2.1.2; 4.3.1
MIL-HDBK	Military Handbook, page ii, 1
NARDAC	Navy Regional Data Automation Center, 4.2.1
NAVDAC	Naval Data Automation Command, page ii, 1; 4.2.1
NDATS	Naval Data Automation Technical Standards, 6.3
NISS	Navy Information System Standards, 6.3
NSO	Network Security Officer, 4.2.2, 4.3.3, 4.3.4, 4.3.5, 4.3.6, 4.4a, 5.8, 5.9.1, 5.9.2
OPNAVINST	Office of the Chief of Naval Operations Instruction, 2.1.2; 4.1.1; 4.2.1; 4.2.2; 4.3
PUB	Publication, page ii, 5; 2.1.2; 4.1.2; 4.3.1;
SECNAVINST	Secretary of the Navy Instruction, 2.3, 4.1.1
SNDL	Standard Navy Distribution List, 5.2a
STD	Standard, 2.1.1
WIN	WWMCCS Information Network, page ii, 4; 4.1.2; 5.1
WWMCCS	Worldwide Military Command and Control System, page ii, 4

4. GENERAL REQUIREMENTS

4.1 Background.

4.1.1 IS security policy. SECNAVINST 5239.2 and OPNAVINST 5239.1A establish the Department of the Navy (DON) IS Security Program and provide guidance on the development and implementation of IS security policies, responsibilities, and procedures for Navy IS activities, systems, and networks.

4.1.2 Network security management. JCS PUB 6-03.7 identifies roles, responsibilities, procedures, and requirements for administration of IS security throughout the WWMCCS community including the WIN. DON uses JCS PUB 6-03.7 as the basis for Navy implementation of network security management because the WWMCCS network environment is similar to and satisfies DON network requirements for user IDs and passwords. JCS PUB 6-03.7 is also the only fully coordinated DOD document that addresses network security management and that defines the roles and responsibilities associated with user IDs and passwords.

4.2 Administration

4.2.1 Automatic Data Processing Security Officer (ADPSO). OPNAVINST 5239.1A requires Navy activities using or planning to use Navy networks to appoint an ADPSO. Activities should formally notify the Commander, NAVDAC (COMNAVDAC) of their ADPSO assignment by providing this information in writing to COMNAVDAC's agent, the Navy Regional Data Automation Center (NARDAC) Newport. NARDAC Newport's address is:

Commanding Officer
Navy Regional Data Automation Center, Newport
Code 53, Building 1A
Newport, RI 02841-5053
Autovon 948-2685, Commercial 401-841-2685

Each ADPSO is responsible for user ID and password administration for all subordinate activity IS sites, including host computer and terminal locations.

4.2.2 Network Security Officer (NSO). OPNAVINST 5239.1A indicates that the NSO designated for each Navy network implements network security primarily through coordination with the activity ADPSOs connected to that network. The NSO also conducts risk assessments to evaluate the security posture of each network component (i.e., host system, terminal, node configuration) and develops a plan to assure that each ADPSO maintains adequate security protection so that network security or reliability is not compromised. User ID and password control in compliance with this handbook should be certified by the NSO for all ADPSOs on the same network.

4.3 Responsibility. The responsibilities outlined below are in accordance with OPNAVINST 5239.1A.

4.3.1 Commander, Naval Data Automation Command (COMNAVDAC). COMNAVDAC is the Program Manager for the Department of the Navy ADP Security Program and the approving authority for Navy networks operating in a multi-level or controlled security mode. COMNAVDAC administers user ID and password control in the Navy within the framework of the DON ADP Security Program. COMNAVDAC also assigns the three position standard user ID site code to all Navy activities, and keeps the user ID series assignments consistent with JCS PUB 6-03.7. A list of ADPSOs is maintained for use within Navy by NARDAC Newport.

4.3.2 Navy activities. The Commanding Officer of each Navy activity appoints in writing a single ADPSO to act as the focal point for all activity IS security matters and sends this information to NARDAC Newport.

4.3.3 Automatic Data Processing Security Officer (ADPSO). The activity ADPSO ensures that proper user ID and password procedures are implemented. The activity ADPSO also maintains complete records of significant transactions and required liaison with other ADPSOs and NSOs.

4.3.4 Network Security Officer (NSO). The NSO ensures adherence to standard security procedures governing network operations and ensures that all ADPSOs in the network have implemented adequate local procedures to protect network security.

4.3.5 Customers and users. Customers and users should comply with all applicable DOD and DON directives and instructions, local standards, and standard operating procedures developed by their NSO or ADPSO.

4.3.6 Contractor(s). Contractors will not connect to a DON computer system or network without prior written permission from the site ADPSO or NSO.

4.4 Responsibilities for Navy networks. The Navy networked environment involves shared responsibilities across Navy activity boundaries. The ADPSO for an activity is responsible for all internal ADP security and coordination with other ADPSOs. Three general roles are identified:

a. Network activity. An activity primarily responsible for the management and authorized use of network resources. Security issues are the responsibility of the NSO.

b. Host activity. The activity responsible for the management of host computers and, as such, is concerned with authorized access to data and computing resources. Security issues are the responsibility of the ADPSO (host ADPSO).

c. User activity. This general category refers to the activity that needs to use IS facilities to support other mission work. Security issues including the proper access and use of IS data and facilities is the responsibility of the ADPSO (user ADPSO).

..5 Information and assistance. Inquiries concerning this standard may be directed to:

a. Telephone: AUTOVON: 288-4452
Commercial: (703) 433-4452

b. Correspondence: Commander
Naval Data Automation Command (Code 14)
Washington Navy Yard, Bldg 166
Washington, DC 20374-1662

5. DETAILED REQUIREMENTS

5.1 Navy standard user ID format. The Navy standard user ID format follows the user ID coding format used on WIN by all DOD services and agencies. This format has been tailored to meet Navy needs and requirements. The following Navy standard coding scheme is used for the 4- to 12-character user ID. The general format, defined and described below, is AAABBBBBBBBB.

5.1.1 Standard user ID site code. AAA is the 3-character standard user ID site code assigned by COMNAVDAC in response to an official request from the ADPSO's activity. See paragraph 5.2 for requesting information.

5.1.2 Standard user ID user code. BBBBBBBBB is a 1- to 9-character code assigned by the ADPSO to uniquely identify a particular user. Personal user IDs are unclassified.

5.2 Standard user ID site code assignment. Upon request, COMNAVDAC assigns a unique standard user ID site code to be used by each ADPSO activity to ensure unique user ID throughout the Navy. ADPSOs or others needing a standard user ID site code must submit a request in writing to: Commander, Naval Data Automation Command, Data Communications Directorate (Code 30), Washington Navy Yard, Washington, DC 20374-1662. To expedite the request for a standard user ID site code, the requesting activity must provide the following information:

a. Full activity name as listed in the Standard Navy Distribution List (SNDL). All Navy organizations should have SNDLs available for use. SNDLs are usually held by secretarial or administrative personnel.

b. Activity short name as listed in the SNDL.

c. SNDL number.

d. Full activity address including zip code (nine digit number if available).

e. Point of contact for this request.

f. Telephone number of the point of contact.

5.3 Standard user ID site code assignment exception. The only exception where a standard user ID site code need not be assigned as a prefix to the user ID is when all the following criteria are met:

a. The requesting user ID must reside in the host at all times and

b. Must be used to initiate activities in the host and

c. Must be used to monitor activities in the host.

5.4 Access request. The IS user must officially request access to IS facilities through the designated user ADPSO. An access request includes the following information:

a. Individual/group. Define the organizational entity requiring access to data or resources.

b. Access category. Describe the method of access desired. Some methods presently used are as follows:

1) Personal user ID and password. Each individual is assigned a unique personal user ID and password that is privately known and maintained. Group passwords are not permitted. The individual is specifically responsible for access. This method is necessary when required by security regulations or when unique data is accessed.

2) Automated (network access) user ID and password. A specially developed device may be inserted between local terminal devices and the Navy network that contains user IDs and passwords. User IDs are not known by the user. Whenever a transmission across a Navy network is necessary, the control device provides an appropriate user ID and password for network access. This method is typically implemented in areas where physical security provides sufficient IS access control.

3) Group user ID. This method is not allowed because group user IDs do not provide individual accountability.

c. Responsible individual. Identify the person responsible for the use of the user ID.

d. Password control. Identify the person responsible for assigning passwords (if other than user ADPSO).

e. Host computers to be accessed. Include the host activity, host computer manufacturer and type, and geographical location.

f. Other. Include other information in the request. For example, the system and database to which each individual has access, or related accounting information.

5.5 User ID assignments. The ADPSO must keep an accurate record of all user IDs assigned, assure uniqueness and standard coding, and forward the respective user IDs to the users and host activities as needed. The user ADPSO is responsible for notifying all concerned ADPSOs whenever the status of a user ID is changed, and verifies that the changes have been made. Host and network ADPSOs are only responsible for maintaining current user ADPSO information.

5.6 Password assignment and control. Each ADPSO is responsible for user ID and password administration and control for all subordinate activity IS sites, including host computer and terminal locations.

a. The ADPSO is responsible for password management within the activity and should consider password generation, distribution to individuals, monitoring use, and reporting abuse and violations.

b. The ADPSO approves the password management methodology for all IS use in the activity.

c. The ADPSO should use FIPS 112 including appendix E of FIPS 112 for password management guidance. Although FIPS 112 states that the appendixes are not mandatory, SECNAVINST 5239.2 makes CSC-STD-002-85, the DOD Password Management Guideline, mandatory. Since appendix E reprints that guideline, appendix E of FIPS 112 becomes a mandatory part of FIPS 112 for the DON.[1]

d. The user ADPSO assigns passwords for the activity. Host and network ADPSOs make provisions to accept and use the user ADPSO assigned passwords. The preferred approach is to supply the user ADPSO with the capability to change the passwords at the network or host level without the intervention of the host or network ADPSO. In cases where host or network systems do not allow user ADPSO assignment, passwords should be forwarded to the user ADPSO for local distribution and management.

e. Passwords should be changed at least every six months. Shorter periods, as needed, may be specified by the ADPSO. All ADPSOs (user, host, and network) should ensure that programs, automated or manual,

---

1. There are differences in the numbering of the sections, paragraphs, and appendixes of FIPS 112 and the DOD guideline. The following key will permit translation of citations so that a citation to the DOD guideline can be found in in appendix E of FIPS 112 and vice versa: The unlabeled foreword to appendix E on page 36 of FIPS 112 combines the foreword and acknowledgments on pages i and ii of the DOD guideline. The unnumbered introduction on page 1 of the DOD guideline becomes paragraph 1 in FIPS 112. Paragraph 1.0, Scope, on page 1 of the DOD guideline becomes paragraph 2, Scope, on page 36 of FIPS 112. This change causes the other paragraph numbers in appendix E of FIPS 112 to be higher by "1" (in the high order position) from the paragraph numbers in the DOD guideline. Thus paragraph 4.1.1 in the DOD guideline becomes paragraph 5.1.1 in FIPS 112. The designations of the six appendixes of the DOD guideline and the paragraph numbers in the appendixes are also changed in appendix E of FIPS 112. Appendixes A through F of the DOD guideline are all part of appendix E of FIPS 112. Appendix A of the DOD guideline becomes appendix E.1 in FIPS 112. Appendix E of the DOD guideline becomes appendix E.5 in FIPS 112. Paragraph A.1 in appendix A of the DOD guideline becomes paragraph 1 of appendix E.1 of FIPS 112. Paragraph E.2 of Appendix E of the DOD guideline becomes paragraph 2 of appendix E.5 of FIPS 112.

are in place to monitor password changes and provide adequate user notification when routine changes occur.

f. Password classification is specified and controlled by the user ADPSO in coordination with other user, host, and network ADPSOs. Password classification alone must not exceed the classification of the data or resources accessed. For example, passwords used to access an unclassified network must be considered sensitive and controlled distribution data, but not confidential.

5.7 User notification. The user ADPSO approves or disapproves the user ID request in writing, including the password management methodology and host access provisions. If approved, the coded user ID is forwarded to the user with guidance for its use on Navy networks.

5.8 ADPSO coordination. The user activity ADPSO coordinates user ID and password control information with the ADPSO for each host site and with the NSO for each Navy network. The host ADPSO assures user ID uniqueness and concurs, where possible, with the user ADPSO password control recommendation. Disagreements in user ID or password administration are adjudicated by COMNAVDAC through the proper chain of command. Host and network resource capacity considerations are beyond the scope of this procedure and are negotiated separately by the user and the resource management organization(s).

5.9 Misuse and vulnerabilities

5.9.1 Abuse and violation. Any suspected abuse or violation noted by any user or host computer site is reported to the appropriate ADPSO and NSO, identifying the user ID involved. Any ADPSO may coordinate the action, but normally the host ADPSO or user ADPSO identified by the first three characters of the user ID is responsible for investigating the violation. In an emergency, any operational command may contact any ADPSO directly. NARDAC Newport maintains an up-to-date directory of all Navy ADPSOs for this purpose. See paragraph 4.2.1 for NARDAC Newport's address.

5.9.2 Resolution. The ADPSO responsible for the site at which a misuse occurs is responsible for resolving the problem in coordination with other ADPSOs. A full report on the problem or violation is made to all ADPSOs involved. A copy of the report is also sent to the NSO.

6. NOTES

(This section contains information of a general or explanatory nature that may be helpful, but is not mandatory.)

6.1 Intended use. This handbook stresses the user ID and password aspects of IS security policies, requirements, roles, responsibilities, and procedures in order to provide Navy IS activities guidance on how to administer and control their user IDs and passwords.

6.2 Issue of DODISS. When this standard is used in acquisition, the applicable issue of the DODISS must be cited in the solicitation (see 2.1.1, and 2.2).

6.3 Navy Information Systems Standards (NISS). The appendix is a list of approved NISS (formerly Naval Data Automation Technical Standards (NDATS)) that is current as of the date of this publication. The approved NISS are also listed in the Naval Supply Systems Command Publication 2002, "Unabridged Navy Index of Publications and Forms" (stock number 0535-LP-004-0100). Copies of the NISS are available from the Naval Publications and Forms Center, 5801 Tabor Avenue, Philadelphia, PA 19120-5099 by submitting DOD Single Line Item Requisition (DD Form 1348) citing the appropriate stock number from the appendix.

APPENDIX

LIST OF APPROVED NAVY INFORMATION SYSTEMS STANDARDS
(formerly Naval Data Automation Technical Standards)

As of 15 Feb 1990

NAVDAC PUB	TITLE	DATE	STOCK NUMBER
17.0A	Introduction and Overview	Apr 1984	0425-LP-100-0800
NAVDAC Advisory Bulletin No. 29 (with NAVDAC PUBs 17.0 through 17.6 as enclosures)		Apr 1982	0425-LP-000-2900
17.0	(Superseded by PUB 17.0A)		
17.1	Procedures for 1401 Conversion Support	Apr 1982	
17.2	Control of Data Processing Installation (DPI) Computer Center Environment	Apr 1982	
17.3	Data Processing Installation (DPI) Problem Tracking System	Apr 1982	
17.4	Standard Maintenance Credit System	Apr 1982	
17.5	Magnetic Tape Interchange	Apr 1982	
17.6	Navy Automatic Data Processing Activities Power Standards	Apr 1982	
17.7B	Microcomputer Software and Hardware Guidelines	Apr 1986 (Superseded by MIL-HDBK-805(OM))	0425-LP-175-3300
17.8A	Navy Data Network Connection Standard	Nov 1984	0425-LP-000-3610
17.9	Procedure for Procuring Public Data Network (PDN) Service	Jun 1983	0425-LP-100-1000
17.10	Network Userid and Password Procedures	Mar 1984 (Superseded by this MIL-HDBK-804(OM))	0425-LP-175-1600
17.11	Document Interchange Format (INTERIM)	Mar 1984 (Superseded by MIL-STD-2002 of 31 Oct 87)	

APPENDIX

NAVDAC PUB	TITLE	DATE	STOCK NUMBER
17.12	Local Area Network (LAN) Planning Standard	Nov 1984	0425-LP-100-1030
17.13	Database Administration Guideline	Oct 1985	0425-LP-100-1040
17.14	COBOL Programming Guideline	May 1985	0425-LP-100-1050
17.15	Microcomputer System Documentation Guidelines	Jul 1985	0425-LP-100-1060
17.16	Guideline for Printed Reports	Sep 1985	0425-LP-100-1070
17.17	Department of the Navy Information System Standards Program (NISSP)	May 1986	0425-LP-100-1080
17.19	Terminal User's Guide for the Defense Data Network Military Network	Aug 1986	0425-LP-100-1100
17.20	Requirements for Terminal Connection of the Defense Data Network (DDN) Military Network (MILNET)	Jun 1986	0425-LP-100-1110
17.21	Automatic Data Processing Site Security	Jun 1986	0425-LP-100-1120
17.22	Initial Graphics Exchange Specification (IGES) Implementation Standard	Sep 1986	0425-LP-100-1130

CONCLUDING MATERIAL

Preparing Activity:
Navy - OM

(Project IPSC-N231)

This page intentionally blank.

STANDARDIZATION DOCUMENT IMPROVEMENT PROPOSAL

INSTRUCTIONS

1. The preparing activity must complete blocks 1, 2, 3, and 8. In block 1, both the document number and revision letter should be given.
2. The submitter of this form must complete blocks 4, 5, 6, and 7.
3. The preparing activity must provide a reply within 30 days from receipt of the form.

NOTE: This form may not be used to request copies of documents, nor to request waivers, or clarification of requirements on current contracts. Comments submitted on this form do not constitute or imply authorization to waive any portion of the referenced document(s) or to amend contractual requirements.

I RECOMMEND A CHANGE:	1. DOCUMENT NUMBER MIL-HDBK-804 (OM)	2. DOCUMENT DATE (YYMMDD) 1990-02-15

3. DOCUMENT TITLE
NETWORK USER ID AND PASSWORD PROCEDURES

4. NATURE OF CHANGE (Identify paragraph number and include proposed rewrite, if possible. Attach extra sheets as needed.)

5. REASON FOR RECOMMENDATION

6. SUBMITTER

a. NAME (Last, First, Middle Initial)	b. ORGANIZATION	
c. ADDRESS (Include Zip Code)	d. TELEPHONE (Include Area Code) (1) Commercial (2) AUTOVON (If applicable)	7. DATE SUBMITTED (YYMMDD)

8. PREPARING ACTIVITY

a. NAME Naval Data Automation Command (Code 14), ATTN: IPSC	b. TELEPHONE (Include Area Code) (1) Commercial: (202) 433-4452,-4734 (2) AUTOVON: 288-4452,-4734
c. ADDRESS (Include Zip Code) Washington Navy Yard, Building 166 Washington, DC 20374-1662	IF YOU DO NOT RECEIVE A REPLY WITHIN 45 DAYS, CONTACT: Defense Quality and Standardization Office 5203 Leesburg Pike, Suite 1403, Falls Church, VA 22041-3466 Telephone (703) 756-2340 AUTOVON 289-2340