Information Management: Organizational Messaging

Defense Message System (DMS)

Security Policies and Procedures

Headquarters
Department of the Army
Washington, DC

History. This is the first issue of this regulation.

Summary. This regulation covers security policies and procedures for DMS as used by the Department of Army (DA).

Applicability. This regulation applies to the Active Army, the Army National Guard, and the U.S. Army Reserve.

Proponent and Exception Authority. The proponent of this regulation is the Director of Information Systems for Command, Control, Communications, and Computers (DISC4). Subject to the reservations set out below, DISC4 has authority to approve exceptions to this regulation that are consistent with controlling regulations and laws. Only the Administrative Assistant to the Secretary of the Army may approve exceptions to authentication, coordination, and proponent authority provisions. DISC4 or the Administrative Assistant may delegate this approval authority in writing to a deputy director in the proponent agency in the grade of colonel or the civilian equivalent.

Interim Changes. Interim changes to this regulation are not official unless they are authenticated by the Administrative Assistant to the Secretary of the Army. Users will destroy interim changes on their expiration dates or when the changes are superseded.

Suggested Improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the U.S. Army Communications-Electronics Services Office, (USACESO), and ATTN: SFIS-FAC-M, 2461 Eisenhower Ave., Suite 1200, Alexandria, VA 22331-0200.

Distribution: Distribution of this publication is made in accordance with the requirements on DA Form 12-09-E, Block XXXX, for Active Army, Army Reserve National Guard, and U.S. Army Reserve.

Distribution.

This printing publishes a new regulation.

By Order of the Secretary of the Army:

Dennis J. Reimer
General, United States Army
Chief of Staff

Official:

J. B. Hudson
Administrative Assistant to the
Secretary of the Army

Table of Contents

Chapter 1 Introduction 1
1-1 Purpose 1
1-2 Applicability 1
1-3 References 1
1-4 Scope 1

Chapter 2 DMS 1
2-1 Overview of DMS 1
2-2 DMS Architecture 1
2-3 DMS Components 1
2-4 DMS Information Assurance Solutions (IAS) Components 2
2-5 DMS Integrations with Existing Network and Security Services 3
2-6 Firewalls 3

Chapter 3 Information Systems Security 5
3-1 Overview 5
3-2 Security Definitions 5
3-3 Overview of Security Issues 5
3-4 Physical Security 6
3-5 Personnel Security 6
3-6 Network Security 6
3-7 Communication Security 7
3-8 Data and Electronic File Security 7
3-9 System/Workstation Security 7
3-10 Identification and Authentication 7
3-11 Virus Prevention 7
3-12 Backup Procedures 7
3-13 Software Security Procedures 7
3-14 Security Assessment 8
3-15 Security Process Overview 8

Chapter 4 Roles and Responsibilities 9
4-1 Local Security Roles 9
4-2 User Responsibilities 10

Chapter 5 IASO and Other Hierarchies 11
5-1 Certification Hierarchy 11
5-2 Approval Roles and Responsibilities 12

Chapter 6 DMS Security Mechanisms 13
6-1 Overview of FORTEZZA 13
6-2 Generation of FORTEZZA Cards 13
6-3 FORTEZZA Security Issues 14

Chapter 7 Certification and Asset Management 14
7-1 Overview 14
7-2 CMI Task Summary 14
7-3 CMI System Security Requirements 15
7-4 Facility Security Criteria 16
7-5 Personnel Security Criteria 17
7-6 Procedural Controls 17
7-7 X.509 Certificate and FORTEZZA Card Management. 18
7-8 Distribution of FORTEZZA Cards and Personal Identification Numbers 18
7-9 CMI X.509 Certificate Security Controls 19
7-10 Audit 19
7-11 Archive 19
7-12 Information System Security Assistance 19
7-13 Asset Security Management 19

Chapter 8 Army Information Technology Security Policies, Control Points, and Requirements 20
8-1 General Security Policy 20
8-2 DMS System Security Control Points 20
8-3 System Security Requirements Specifications (SSRS) 21
8-4 General DMS Security Requirements 21
8-5 Minimum Army DMS Security Requirements 22
8-6 DMS Administrative Requirements 22
8-7 Automated Information System Security Procedural Requirements 23
8-8 Data Integrity 23
8-9 Data Continuity 24
8-10 Continuous Protection 24
8-11 Additional Security Requirements 24
8-12 Labels 24
8-13 DoD Detailed Specifications 25

Chapter 9 Mobility And Security Issues 29
9-1 Change to DMS Components 29
9-2 Remote or Portable Information Technology Systems 29
9-3 Temporary Duty 29

Chapter 10 Setting a Security Policy 29
10-1 Overview of Policy Requirements 29

Chapter 11 Security Training 30
11-1 Security Training for the IASO 30
11-2 Security Training for Users 30

Chapter 12 Assessing and Responding to Threats 30
12-1 Risk Management 30
12-2 Vulnerability Analysis Assessment Program 31
12-3 Information Assurance Vulnerability Alert (IAVA) 31
12-4 Types of Attack 31

Appendix A – Acronyms A-1

Appendix B -- Glossary B-1

Appendix C – References C-1

Appendix D – Security Features User's Guide D-1

Chapter 1 Introduction

1-1 Purpose
This document describes basic security policies and procedures for Army security personnel working with the Defense Message System (DMS) version 2.1.

1-2 Applicability
This policy does not supersede the approval process implemented for AUTODIN components and systems. As long as AUTODIN components are functioning, the security policies and procedures required in the DMS Component Approval Process (DISA letter 24 March 1993) remain necessary and will continue to govern the connection of DMS transitional and legacy components to AUTODIN. This policy does supersede the 10 December 1993 and the January 2000 DMS Security Policy documents.

1-3 References
A full list of references is in Appendix C.

1-4 Scope
The DMS is interfaced with the existing Defense Information Infrastructure (DII) network and existing legacy networks. Therefore, there is no clear delineation between general network security issues and DMS security issues. For the sake of this document, DMS security is contained within the broad scope of general security.

Chapter 2 DMS

2-1 Overview of DMS
a. *Version and Purpose.* DMS Version 2.1 provides electronic delivery of messages within the Department of Defense (DoD) and intelligence communities for organizations and individuals. The DMS is intended to provide messaging and directory services to all strategic and tactical users, access to and from worldwide locations, and an integrated interface to other U.S. Government, Allied, defense contractors, and other authorized users.

b. *What Comprises DMS?* It is a flexible, commercial-off-the-shelf (COTS)-based network system providing messaging and directory services which are capable of taking advantage of the flexible and expandable DII network. The DMS encompasses hardware, software, procedures, standards, facilities, and personnel. Security services provided in support of the DMS protect all data transmitted, stored, or processed by the systems for all levels of sensitivity and classification.

2-2 DMS Architecture
The DMS Architecture enables organizations to implement DMS services in accordance with operational requirements. The key aspect of the DMS architecture is its support of the multiple levels of security assurance and grades of messaging service.

a. *Grades of Service.* The high grade, high assurance messaging–service is associated with the X.400 system, while the lower grade, lower assurance messaging service is associated with the Simple Mail Transfer Protocol (SMTP) system.

b. *Security Between Grades.* Within each of the grades of service there is a possible range of security assurance levels: high (hardware FORTEZZA), lower (software security such as software FORTEZZA or commercial security), and none (passwords only). The no-security assurance level should only be looked upon as a transitional capability, rather than a target. Target DMS implementations should include some level of security protection for all messaging.

c. *DMS Security Domains.* There are three domains for full DMS implementation: Unclassified, SECRET, and TOP SECRET. The Secure Network Server (SNS) distinguishes between the varying levels of security environments. The Trusted Workstation is the security solution for classified domains.

2-3 DMS Components
Below is a brief list of the components used in DMS version 2.1. For more detail on these components and their function, see Letter of Instruction AR-25 Ops.

a. *User Agent (UA).* The UA is an email application on the user's computer that provides the ability to compose, send, and receive messages.

b. *Mail List Agent (MLA).* The MLA is required to simplify the distribution and management of messages to multiple recipients. When an Address List (AL) is used, the Message Transfer Agent (MTA) sends the message to the MLA, which makes and sends a copy of the message to each of the addressees for the AL. The MLA processes messages that contain ALs only.

c. *Message Transfer System (MTS).* The MTS is the collection of the logically interconnected MTAs in the system.

d. *Message Store (MS).* The MS software provides a mailbox where messages are delivered when the UA is not available. The MS accepts messages from the MTA on behalf of the UA, and stores the messages until the UA returns to service.

e. *Multi-Function Interpreter (MFI).* The MFI is the gateway used to interface messages from users to existing (legacy) networks such as AUTODIN, Simple Mail Transfer Protocol (SMTP), COTS email packages, Allied message systems, and other existing X.400 networks. When outgoing encrypted messages are prepared to leave DMS, they are decrypted at the MFI.

f. *Profiling User Agent (PUA).* The PUA is a UA capable of re-distributing a message based on its subject, contents, and key words.

2-4 DMS Information Assurance Solutions (IAS) Components

The DMS incorporates security solutions and components developed under the IAS. The National Security Agency (NSA) developed IAS and the Message Security Protocol (MSP) to protect information in unclassified and classified domains. The architecture is the basis for meeting detailed IAS-compliant component specifications and for system level Security Test and Evaluation (ST&E) and integration and will facilitate Certification and Accreditation (C&A).

a. *Certificate Authorization Workstation (CAW).* The CAW is NSA's special purpose trusted workstation used for the generation, management, and distribution of keying material and X.509 Certificates. The CAW initializes the FORTEZZA card, generates the keying material and associated certificate, and stores them on the FORTEZZA card. The CAW interfaces with the ADUA to post the X.509 Certificate, which includes public key material, to the X.500 Directory. Also, individual user privileges are programmed on the FORTEZZA card, which include the following:
   - **Certificate Type** (Individual, Org. Firstborn, Org. Sibling, etc.)
   - **KEA Clearance** (Top Secret, Secret, Confidential, and Unclassified)
   - **KEA Communications Privileges** (Critic/Flash, Immediate/Priority, Routine/Deferred, or Multifunction Interpreter)
   - **DSS Signature Privileges** (Org. Release Authority or Read Only)

b. *FORTEZZA Card.* The FORTEZZA card is a PC Memory Card International Association (PCMCIA) card that provides the high assurance cryptographic services to the DMS applications. These cards are rugged, credit card-size peripherals that add capabilities to computers. The FORTEZZA card stores a user's private keys (Key Exchange Algorithm [KEA] key and Digital Signature Standard [DSS] key) and public certificate. The private keys and public certificates are used to support digital signature operations and message encryption.

c. *Mail List Agent.* The MLA provides a collective addressing capability for DMS. This function allows a message originator to have messages delivered to a pre-defined group of recipients by addressing a single entity (the mail list). Mail lists may be in the X.500 directory or stored in the MLA. The MLA removes all the MSP security tokens and replaces them with security tokens needed by the ML members to access the message contents. The MLA requires a FORTEZZA card for operation.

d. *Address List.* Address lists are not components, but they still have IAS security controls. The AL used by the MLA is considered classified if at least one address in the composition is classified as CONFIDENTIAL or higher. If an AL is unclassified and it is necessary to send a classified message to the AL, the message text is marked in accordance with AR 380-5, but the AL, itself, is not classified.

e. *Profiling User Agent.* The PUA provides an organization with the capability for onward delivery of incoming messages. Once the PUA receives an incoming message, it automatically redistributes the message to the appropriate parties based on the contents of the message and the distribution profile that has been established by the recipient organization. Software enhancements provided in DMS release 2.1 enable the PUA to support multiple organizations. The PUA requires a FORTEZZA card for operation.

f. *High Assurance Guard (HAG).* The HAG provides guard services between domains of different security levels. The HAG is comprised of hardware, software, and FORTEZZA. The HAG is designed to filter message traffic before transmission between classification levels (i.e., Secret, Unclassified).
   (1) *Messaging Between Domains.* The HAG ensures messages released from a higher classification domain have been properly labeled and protected before message transfer to the lower classification domain. The HAG also enforces access controls for messaging from the lower domain to the higher; this mechanism can also protect the higher domain from attacks based in the lower domain. Message transfers between users within the same classification domain located on the same network will not need to go through the HAG.
   (2) *SPECAT.* Legacy system users should note that current DMS products do not support Special Category (SPECAT) messages. SPECATs are prohibited from entering DMS and must be processed by legacy systems.
   (3) *Location.* The HAG should be physically located within a protected area that is commensurate with the highest classification level of the network(s) to which it is connected.

g. *Firewall.* A firewall is an access control gateway used to establish a protected environment and

encompasses all components within a protected enclave such as an agency's site. Firewalls enhance network and application security. Services and agencies implement firewalls in accordance with their own network security policy. However, when those firewalls are located between the local DMS enclave and the DMS backbone infrastructure, DMS operation and systems management can be affected.

2-5 DMS Integrations with Existing Network and Security Services

DMS is being deployed within existing site network infrastructures that provide many other services beyond messaging. In order for DMS to achieve its full potential it has to co-exist within the boundaries defined by a site's operational needs. This section identifies areas where DMS may interact with or impact existing network services.

a. *Domain Name Services.* The Domain Name Service (DNS) is used within the DMS environment to provide mappings between host names and IP addresses. In DMS version 2.1, given a Host name, DNS can be used to provide the IP addresses of DMS components; in previous releases the IP addresses were hard-coded into the components. However, DMS components retain the capability to be configured to use IP addresses exclusively. It is highly recommended that DNS be used within DMS. Sites that choose to use IP addresses create a significant management burden to the DMS infrastructure as well as other DMS sites because these locations will have to manually maintain the IP addresses of the non-DNS sites within their DNS.

(1) DNS consists of two parts:

- DNS name servers, which maintain the databases holding the mappings between the host names and the IP addresses, and
- DNS clients, which query DNS name servers with requests to resolve host names to IP addresses. The DNS name servers that comprise the DNS infrastructure are not part of the DMS. Rather, the DMS components use existing DNS name servers (part of a location's network infrastructure) to provide the name to IP address lookup/resolution.

b. *DMS DNS Components.* DMS components include DNS clients to query DNS name servers operated by a non-DMS organization. Each DMS component using DNS supports querying both a primary and secondary DNS name server. At a minimum, two DNS name servers are configured for each DMS component to ensure that there is not a single point of failure. Without access to a DNS name server there is no way for a DMS component configured to use DNS to convert a host name to an IP address.

c. *Specification of Servers.* Version 2.1 of DMS does not include the specification of DNS name servers. DMS takes no part in DNS administration other than to make its products compatible with existing (NIPRNET, SIPRNET, etc.) DNS services. DMS components are simply assigned local domain names integrated into the existing DISN DNS structure. No DNS server is the responsibility of DMS. No domain name structure specifically relating to DMS is required. DMS host names will have to be registered in accordance with local registration procedures.

d. *Configuration of Host Names.* The use of DNS to allow administrators to configure DMS products based on host names relieves administrators of the problem of maintaining numeric network addresses in component configurations. The use of host names simplifies administration of DMS components, especially in the case of network re-configurations which result in IP address changes. The configuration of DNS name servers and the caching of DNS information locally may help reduce performance impacts. While the DNS name server infrastructure is outside the scope of DMS, the establishment and location of name servers could cause performance impacts. The placement of DNS name servers and the configuration of DMS components to query both a primary and secondary name server are critical to the successful deployment of DNS-capable systems. Name servers need to be located logically close to the DMS components which will access them. Furthermore, each DMS component needs to be configured to search at least two name servers which are geographically separated to provide adequate redundancy and availability. The DNS infrastructure will be installed and maintained by a third-party provider.

e. *DNS and SMTP.* DNS is also used by SMTP for address resolution of a mail host within domains. Mail Exchange type records are used by the DNS to identify SMTP mail servers for a DNS domain. A separate Address type (A) record must also exist for each mail server. Most DNS implementations support multiple MX records with a preference setting to identify the primary vs. alternate servers. When configuring the DNS, use the format: [SMTP domain] IN MX [preference value] [mailserver name].

2-6 Firewalls

a. *Overview.* This section addresses considerations for deploying DMS in a network environment that contains commercial firewalls. In brief, this requires defining the protocol and IP port usage for each DMS component logical connection that must cross the firewall. For some of standard Internet protocols (ftp, snmp, telnet) used by DMS,

commercial firewalls may provide an application proxy. For most DMS protocols (X.400 P1, DAP, DISP, DSP, LDAP) and RPCs. However, commercial firewalls do not provide application proxies; therefore, their generic plug proxy must often be used.

b. *Recommended Configurations.* In general, it is anticipated most sites will fall into the case where a firewall will be placed at a DMS site to isolate a protected enclave of DMS components from the wide area network (NIPRNET or SIPRNET), i.e., a local site's DMS components will all be placed behind the firewall, including the Primary Groupware Server (PGWS). This architecture is recommended in order to limit the number of DMS-relevant protocols that a COTS firewall would have to pass to a set for which reasonable security assurance could be applied. (These are discussed below.) Some sites may require alternate configurations such as a UA on the opposite side of the firewall from its GWS. During detailed design, each logical connection, both in-bound and out-bound, that must traverse the firewall must be identified and validated against local security policy. This information is needed for review with the site security administrator and for the firewall administrator to configure the firewall.

c. *Recommendations.* The recommendations identified in this section are derived from the architecture specified and the DMS protocol support needs identified in the SDD Firewall Report 1, *DMS Component Interactions, Services & Protocols*. Firewall Report 1 provides the following additional recommendations:

- Within a protected enclave, local time sources should be used to provide time synchronization for DMS components.
- Management of a site's DMS components should be performed using a local MWS.
- Communications between Groupware Servers (GWS) and their clients, using either P7 or proprietary protocols, should be confined to the enclave, i.e., not traverse the firewall.

d. *Protocols.* Firewall Report 3, *Recommended DMS Architectural Solutions for Firewalls,* identified those DMS protocols that are required to be passed through the firewall at all times and others that are only passed in the event that an alternate component at a regional or global site, such as a Management Workstation at a Regional Operations Security Center or a Global Directory Service Agent at a Regional Node, must temporarily substitute for a failed primary component. The required protocols are P1, SMTP, DISP, DSP, and FTP. The protocols that must additionally pass through in backup mode are DAP and SNMP. The necessity of these selections is described below. Because some of these protocols are OSI application protocols, which require services from OSI upper layer protocols, application gateway firewalls must also support RFC 1006.

e. *Remote Procedure Calls (RPCs)* create significant security problems for Application Gateway firewalls (described in Firewall Report 1), and, therefore, passing RPCs through this type of firewall should be avoided. In the event that an Application Gateway firewall at a site where DMS components must also be installed is configured so that DMS client UAs must be located on opposite sides of the firewall from its associated Groupware Server, another architecture alternative must be considered.

f. *Other Firewall Interface Issues.* Additional firewall issues can be derived from the DMS functionality requirements specified for all DMS components. These firewall functionality requirements include DMS compliant DSAs and MTAs, support for FORTEZZA, and support for DAP. Commercial firewall implementations currently in use do not support any of these requirements, and few commercial offerings have plans for upgrading to FORTEZZA or DAP support. Currently, none has plans to incorporate DMS-compliant DSAs or MTAs.

g. *COTS Gateways.* In addition, most COTS Application Gateway firewalls do not have support for OSI X.400 and X.500 protocols. For DMS Site environments where firewalls already exist that do not support X.400 and X.500 protocols, other firewall capabilities (e.g., plug_gw) or other architecture alternatives (e.g., filtering router) must be considered. See SDD Firewall Report 2*, Defense Message System Commercial Firewall Study*, and Firewall Report 3 for details.

h. *Application Gateway Firewalls.* RPCs create significant security problems for Application Gateway firewalls (described in Firewall Report 1), and, therefore, passing RPCs through this type of firewall should be avoided. In the event that an Application Gateway firewall at a site where DMS components must also be installed is configured such that DMS client UAs must be located on opposite sides of the firewall from its associated Groupware Server, another architecture alternative must be considered.

i. *Dial-Up Connectivity.* The DMS Remote user (dial-up) connectivity solution is not affected by Firewalls. A Firewall provides network-level access security, dial-up is via communications servers, which are "behind" the firewall. It is assumed that the communications server provides the requisite security.

Chapter 3 Information Systems Security

3-1 Overview

The fundamental security requirements are:

- Protection of data from unauthorized disclosure, modification, or deletion, particularly messages and directory information;
- Protection of services and resources from unauthorized use and denial of service;
- To verify the identity of appropriate users; and
- Establishment of accountability to individual persons, entities, or processes.

Secure operation depends on accurate and consistent enforcement of confidentiality, data integrity, resource availability, and accountability for actions.

3-2 Security Definitions

The following terms are used to describe aspects of security.

a. *Confidentiality.* Confidentiality is the control of access to and dissemination of information so that the information is protected against unauthorized disclosure. Confidentiality is provided through the encryption of messages when they are sent from the originator (writer) to the recipient (reader). This is called writer-to-reader confidentiality.

b. *Data Integrity.* Data integrity is the protection of messages against unauthorized modification. Data integrity is a means for the reader of the message to verify that the received message is the same as the source message, through the use of digital signatures. This is called writer-to-reader integrity.

c. *Non-Repudiation*. Non-repudiation is a service which protects against users denying that they participated in a message exchange when in fact they did. Non-repudiation takes two forms: non-repudiation with proof of origin and non-repudiation with proof of delivery. Digital signatures are used to provide either form of non-repudiation. Non-repudiation with proof of origin is fulfilled by having the originator digitally sign the message. Non-repudiation for proof of delivery is provided by having the recipient return a digitally signed receipt.

d. *Identification and Authentication (I&A).* Identification is the assertion of identity by a person or process. Identification is established during logon by entering the user ID. Authentication is the mechanism used to prove that the entity (person, process) has furnished a valid identity. Simple authentication is performed by using a password supplied by the user during the logon process. Additional forms of authentication are described in the next two paragraphs.

e. *Enhanced Authentication.* Enhanced authentication requires users to provide a FORTEZZA card and entering a Personal Identification Number (PIN) in order to activate the features of the card. This is called enhanced authentication because the users must provide two proofs of identity: They must both have the card and know the PIN. Access to components is restricted to those persons who have a valid FORTEZZA card and PIN.

f. *Strong Authentication.* The purpose of strong authentication is to provide one party in an exchange of information with high confidence that the other party has given a valid identity. There are two forms of strong authentication:

(1) *Per-Message Authentication.* On a per-message basis the digital signature capability provides assurance that messages originate from the user who claims to have originated it. Only that user/FORTEZZA card combination can sign the message with that user's private key. If the signature produces the correct message hash, the recipient has strong authentication for that message.

(2) *Bind Authentication.* The second form of strong authentication is to establish authentication at bind time, when a session between two entities is created, and to have the authentication be considered valid as long as the integrity of the session persists. This form is also called persistent verification.

g. *Access Control.* Access control refers to the mechanisms used to ensure that only authorized users gain access to the system resources. These mechanisms vary in type and technique depending upon the resources being protected. For example, physical possession and knowledge of the associated PIN is required to invoke a FORTEZZA card.

h. *Auditing.* Auditing is the collecting, safekeeping, and reviewing of records of system activity that allows the tracing of individual activities with respect to the adherence to security policy. This includes gathering reliable information that aids in the discovery and investigation of violations or attempted violations of security policy, technical attacks oriented toward denial of service, and loss of system or information integrity.

3-3 Overview of Security Issues

Several different types of security issues combine to cover all aspects of Information system security. These sub-issues include:

- Physical Security
- Personnel Security
- Network Security

- Communication Security
- Data Security
- Electronic File Security
- System/Workstation Security.

3-4 Physical Security

No system is secure if its components can be compromised. Each component or suite of components must be protected with a physical security policy and procedure commensurate with the highest classification of the information processed by that component or suite. At its simplest, physical security will be ensured by protecting supplies, power sources, furniture, equipment, rooms, and buildings. They are protected with adequate locks, card keys, guards, sign-in books, and paper shredders.

a. *Access control.* Complete physical security requires a series of access controls preventing unauthorized access to components. Procedures will include a means of assuring that data and materials are safe from unauthorized use and that users will have access only to those resources or data for which they are cleared and authorized to use. Physical security processes should not impact availability of the system to authorized users. Access policy issues include:
   - Data, services, and resources shall be available for use by authorized users to the capacity of the system.
   - Prompt notification of non-delivered messages.
   - Protection against denial-of-service attacks.
   - A warning system to alert users of degradation of system capacity.
   - Prevention of accidental or deliberate attempts by users to make the system unavailable to other users.
   - Prevention of unauthorized modification or deletion of configuration information.

b. *Types of Controlled Access.* There are two types of areas requiring controlled access: controlled areas and restricted areas. The access control indicators for these areas are set in the site DSAs by the appropriate registration personnel.
   (1) *Controlled Areas.* Controlled areas are those areas allowing access to nonsensitive or noncritical but sensitive data. The area defined includes the rooms housing the DMS equipment, program files, computer maintenance areas, data storage libraries, power systems, and supply storage areas. Access controls to Controlled areas should be set to prevent entry by unauthorized persons.
   (2) *Restricted Areas.* Restricted areas are any housing critical-sensitive equipment, software, or information. Access controls to restricted areas should limit entry to only those persons specifically listed on the access control list. Any personal not authorized for access who are required to enter the restricted area (e.g., maintenance personnel) shall be escorted at all times.

3-5 Personnel Security

General requirements for personnel security are outlined in DoD 5200.2-R, Personnel Security Program and DISAI 240-110-8. DMS personnel are defined as anyone directly involved with DMS, including message originators, message recipients, system operators, system administrators, accounting personnel, registration and certificate management personnel, installers, maintainers, and security officials.

a. *Types of Clearance.* All personnel must have a clearance level that is as high or higher than the classification level of the information they have access to. Personnel who have access and authorization to change any DMS hardware or software must have a clearance level that is as high or higher than the classification of the components changed.

b. *ADP Levels.* DoD 5200.2-R states that DoD personnel and contractors must be assigned to one of three position-sensitive designations:
   (1) ADP I is a critical-sensitive classification. ADP I personnel are responsible for planning and implementing computer systems and security programs.
   (2) ADP II is a noncritical-sensitive position. ADP II personnel are also responsible for planning, designing, operating, and maintaining computer systems. ADP II personnel report to ADP I personnel.
   (3) ADP III is a nonsensitive classification, used as a blanket classification for all personnel who are not rated ADP I and ADP II.

3-6 Network Security

All linked computers must have established procedures for protecting data integrity and security for any information available on the network. These procedures must correspond to the highest level of classification of any data on any computer in the network. General network security issues include:

- Use of proper I&A encryption technologies at every point of interconnection to another network,
- Disallowing direct connections between the network and the Internet,
- Preventing any connection at all between a classified network and the Internet,
- Preventing transmission of classified or sensitive information over unsecured lines, and
- Use of proper firewalls and I&A procedures for remote users.

Network security policies should include the following considerations:

- Host-Based Host Security
- Host-Based Network Security
- Network-Based Network Security

- Threats to Network Security.

a. *Host-Based Host Security.* Host-Based Host Security ensures the host computer against unauthorized access from users or Local Area Network (LAN) connections. Host-Based Host Security policies cover password protection and restrictions, virus protection, unauthorized user access or privileges, and attack by password-guessing programs. Specific programs include but are not limited to Tripwire, Crack, and Computerized Oracle Password Systems (COPS).

b. *Host-Based Network Security.* Host-Based Network Security is aimed at the security of network utilities. Host-Based Network Security policies cover attempts to disable or restrict the Host's network services, appropriate filters for incoming network requests, and procedures for File Transfer Protocol (FTP) requests to the host or network.

c. *Network-Based Network Security.* Network-Based Network Security covers all policies for network security that do not directly involve the host. This includes but is not limited to gateways and firewalls. Networks must be secure from physical or electronic access by unauthorized individuals.

d. *Threats to Network Security*. DMS is vulnerable to the same threats that could damage any Automated Information System (AIS). These threats include but are not limited to:
   - Sabotage
   - Denial of Service attacks
   - Introduction of false data
   - Modification or deletion of data
   - Unauthorized access to secure hardware or software.

3-7 Communication Security

Communication security requires the use of trusted products in the DMS system, including approved modems, LANs, routers, satellites, and other equipment. Communications security policies must prevent both unauthorized access to classified communications and the validity of the messages on the system. Therefore, policies for communication security must also cover the issues of cryptosecurity, transmission security, emissions security, and the physical security of messaging components.

3-8 Data and Electronic File Security

Data and Electronic File Security protect sensitive information from access by unauthorized individuals or inappropriately modified by authorized users. Security policies shall, therefore, protect the integrity, availability, and confidentiality of data. The privacy of tangential information that could be used to compromise classified information must also be protected. This includes such items as personnel information (which should be considered sensitive data) and Privacy Act data. Both data security and electronic file security require policies that shall enforce:

- Protection of data from access or modification during processing, transmission, and storage;
- Prevention of unauthorized disclosure of data during processing;
- Limiting access to data that has been re-allocated; and
- Verification processes for users' digital signatures.

3-9 System/Workstation Security

System/Workstation security is the responsibility of the individual users. Their responsibilities are listed elsewhere in this document.

3-10 Identification and Authentication

All sensitive systems will control and limit user access based on the I&A of the user. I&A ensures accountability can be established and maintained based on unique, non-forgeable security tokens. Non-repudiation allows users to know that a message has reached the intended recipient and protects against users denying their participation in a message exchange. The most common method for implementing I&A is via a user ID and password. All requests for system accounts will require I&A. The identity of each user must be established before authorizing system access, and each user must have a unique ID.

3-11 Virus Prevention

Computer viruses pose a significant threat to computer systems. A virus is defined as any program or partial program that modifies programs, executes commands, or damages hardware or software. Viruses can replicate themselves to "infect" other programs or computers. The attack and infection can happen within a very short time but can cause serious damage to programs, data, or equipment. To prevent this damage, the following steps shall be taken:

a. All components will be equipped with up-to-date anti-viral software.

b. All diskettes will be scanned and certified virus-free before use.

c. All new software will be scanned and certified virus-free before use.

The individual user's responsibilities in virus protection are listed elsewhere in this document.

3-12 Backup Procedures

The Information Assurance Security Officer (IASO) or LAN administrator is responsible for establishing system backup schedules. The frequency of the backups will be determined by the sensitivity of the data on the system. Full system backups should be made on a regular basis, such as weekly, monthly, or quarterly. Backup media must be properly labeled, dated, and stored in a secure location. If necessary, a second set of backup media shall be stored off-site.

3-13 Software Security Procedures

Authorized software is software that is pre-installed by the Office of Information Resource Management or by

designated AIS personnel. Locally purchased software should not conflict with service-wide software, be approved for use, be scanned for viruses before installation, and be properly licensed.

3-14 Security Assessment

Although there is an official Risk Assessment program that is performed every 3 years or upon significant system change, site security should be continually evaluated and accessed, per AFWIC Security Assessment for DMS 2.1. Ongoing security assessments should look for the following insecure conditions:

a. *Unnecessary Services Enabled.* Only four service protocols are required to run with DMS:
   - FTP
   - TELNET
   - TFTP (on separate private sub-nets for X-terminals)
   - SNMP (blocked at firewall, and restricted by a password)

   Any others, such as SENDMAIL, FINGER, IRC, and the like should be disabled.

b. *Unrestricted Access to Systems*. Unix boxes are to be kept in "trusted mode" and "r" services should be disabled.

c. *Poor passwords.* An easily broken password is not secure. Below are a list of password requirements. Refer to the Site Security Operational Procedures written by the IASO for more information.
   (1) Key aspects of a strong password are:
      - A mix of alpha-numeric characters with one special character
      - 12 characters in length
      - no dictionary words, proper names, etc.
   (2) The password policy also defines the lockout policy. In general, the system should lock a user out after 3 incorrect log-in attempts.
   (3) Finally, all default passwords should be treated as insecure and immediately changed.

d. *Poor Configuration Control.* Inconsistent account policies and unrestricted user access to the registry are security violations. To prevent them:
   - Inactive accounts should be removed and/or deactivated
   - File permissions should be scrutinized
   - Audit logs should be run, read, and kept
   - Root privileges should be minimized
   - Access privileges and shared directories should be limited

3-15 Security Process Overview

No single security measure can adequately protect a system as complex as DMS. Fortunately, design changes in DMS version 2.1 address over 85% of the previous system's vulnerabilities, and Maintenance Release 3 will add even more security features while simplifying system installation and administration. A layered security approach is used to provide Information Assurance and lock down a DMS server. The basic layers are listed below. For more information, see the Operations Working Group Security Briefing.

a. Operating System (OS) Installation
   - Subset of OS functions
   - OS hot fixes

b. Product Installation
   - User/Admin accounts
   - SMNP agent configuration
   - Product hot fixes

c. Security FEN. Remove excess:
   - Services
   - File permissions
   - Access controls

d. TFM
   - Password policy

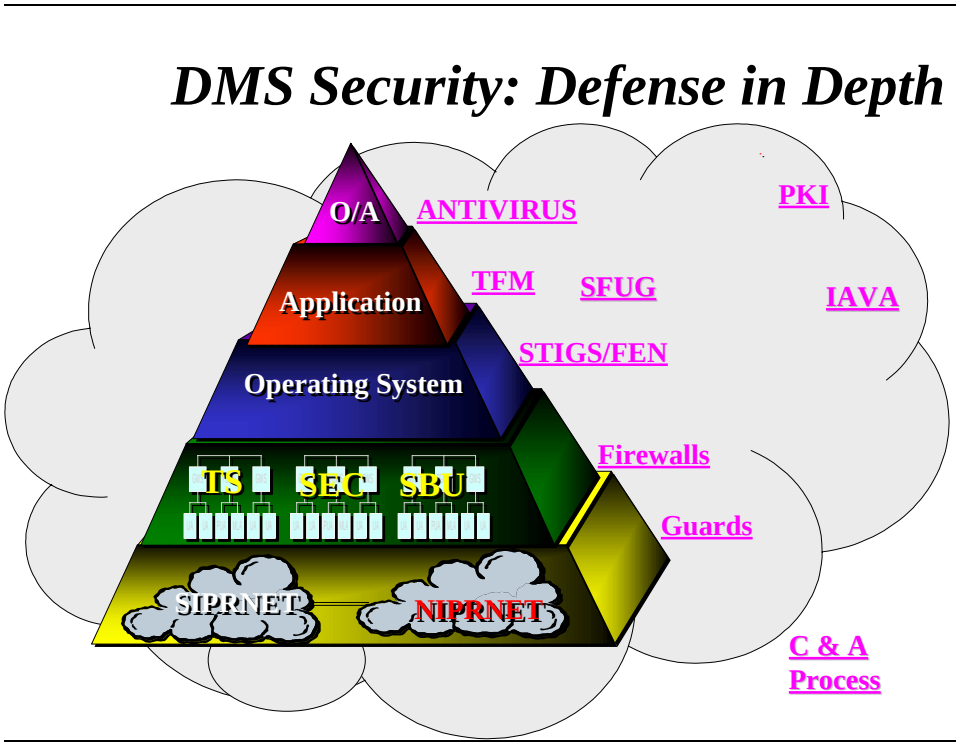


Figure 4-1. Defense In Depth

Chapter 4 Roles and Responsibilities

4-1 Local Security Roles

The duties and responsibilities listed below are the most critical to the success of life cycle security management and are not meant to describe every possible security role at a local site.

a. *Designated Approval Authority (DAA)*. The Local DAA is the management official tasked to determine the level of acceptable risk for all information systems and issuing an accreditation statement if the risk level is acceptable. With the accreditation statement the DAA formally accepts security responsibility for the operation of the system. The DAA's other responsibilities include:

(1) Reviewing and approving security safeguards;

(2) Ensuring that security training is available

(3) Ensuring that data ownership, accountability, access rights, and other security concerns are established for each information system; and

(4) Ensuring that all suspected security violations are documented, reviewed, and reported by staff.

b. *Information Systems Security Manager.* The ISSM ensures that program requirements are implemented, but the ISSM does not participate in daily operations The ISSM is not permitted to share roles with the IASO, Network Security Officer (NSO), or Systems Administrator (SA). The ISSM's responsibilities include:

(1) Ensuring that an infrastructure is in place to implement daily security operations;

(2) Ensuring that all systems operate with an acceptable level of risk;

(3) Ensuring that all information security incidents are properly reported, investigated, and resolved;

(4) Ensuring the development of a security training program for all personnel; and

(5) Ensuring that the appropriate information security tools are disseminated and used.

c. *Information Assurance Security Officer.* An IASO can be appointed for information systems or workstations. At some installations, the IASO may be in charge of systems outside DMS as well. The IASO must receive and maintain the Information Assurance certification, as indicated in the DA PAM 25-IA. The IASO will implement the ITSEC policies on behalf of the ISSM. The IASO's responsibilities include:

(1) Developing local security procedures and publish a site-specific Security Features User's Guide (SFUG);

(2) Administering user accounts and assigning passwords;

(3) Meeting all appropriate training requirements;
(4) Ensuring all CERT notifications are acknowledged and the results are forwarded to the ISSM;
(5) Providing user security awareness training;
(6) Maintaining an inventory of all DMS hardware, software, and functional application systems;
(7) Conducting and documenting the site DMS Risk Assessment
(8) Coordinating system security matters with users and the DMS Security management structure;
(9) Monitoring system activity for security violations;
(10) Assisting in implementing, developing, and testing the site DMS Contingency Plan;
(11) Establishing and maintaining a list of all authorized system users;
(12) Verifying that each user is appropriately authorized and cleared;
(13) Monitoring local compliance with security procedures;
(14) Assigning security privileges and access controls of CAW users
(15) Performing a CAW audit, archiving, and deleting as necessary;
(16) Performing review and deleting audit logs;
(17) Ensuring systems are developed, operated, and maintained per AR 25-IA and DA PAM 25-IA;
(18) Reviewing and evaluating the security impact of system changes;
(19) Ensuring that training and certification of users also extends to users of remote or portable equipment;
(20) Accrediting portable information systems such as laptop computers or Personal Data Assistants, as required, according to AR 25-IA and DA PAM 25-IA;
(21) Ensuring proper control of FORTEZZA cards; and
(22) Investigating loss and/or destruction of FORTEZZA cards.

d. *Network Security Officers.* An NSO will be appointed to implement the Information System Security Program for each network. The NSO's duties are similar to the IASO's, except that the NSO is responsible for networks rather than individual systems. The NSO and the IASO roles can be filled by the same person. NSO responsibilities include:
(1) Ensuring network compliance with information system security procedures;
(2) Installing, managing, and monitoring all tools associated with network security, including firewalls, virus detectors and the like;
- Developing and maintaining network security procedures; and
- Working with SAs to ensure implementation of CERT notifications.

e. *System Administrators.* SAs are responsible for daily monitoring of system resources. The roles of the IASO and the SA are usually filled by the same person. The SA's responsibilities include:
(1) Assisting the IASO (if not the same person),
(2) Administering user I&A mechanisms,
(3) Conducting system audits, and
(4) Correcting vulnerabilities exposed by risk assessment tools and reporting to IASO (if not the same person).

f. *Security Manager (SM).* The SM is responsible for the administration of security programs. The SM's responsibilities include:
(1) Serving as a focal point for advice, assistance, and distribution of security policies and the status of security investigations;
(2) Implementing security education and training;
(3) Reporting security violations; and
(4) Ensuring that assorted security briefings are conducted.

4-2 User Responsibilities

Individual users are responsible for using the appropriate safety procedures to protect their workstations and data from corruption or attack. Users are also responsible for complying with all security policies, completing security training, reporting any incidents to their supervisors, and providing input to surveys and documentation when requested.

a. *UA User Responsibilities.* The user may configure certain DMS UA security features. They include whether or not entering the FORTEZZA card PIN is required for each message, the length of time before the FORTEZZA card times out when idle, certain audit features, configuring UAs for directory searches, and user selection of the DMS UA password. General guidance for configuring UAs for directory searches and user selection of the DMS UA password is given below. The user should reference local security policy and procedures for guidelines for other DMS UA configuration. It is important for the user to follow local security policies when performing any configuration of the DMS UA. It is also important that the user not alter the initial DMS UA configuration unless specifically authorized to do so by local security policy.

b. *Routine Safeguards.* The following routine safeguards shall always be used:
(1) All accounts will be properly password protected.
(2) Users will log off of workstations before leaving them unattended.

(3) Users will perform any required backups of their workstations and keep the backup materials in a safe place.
(4) Keyboards should be equipped with keyboard locks and workstations with time-out screen savers.
(5) Diskettes will be set to write-protect.
(6) Workstations will be protected with surge protectors.
(7) Workstations and diskettes will be protected from such hazards as food, drink, and magnetic devices.
(8) Property passes will be obtained for the relocation or removal of any equipment.

c. *Identification Safeguards.* All sensitive systems limit user access based on the user's I&A. The user is responsible for safeguarding the item used for authentication. Examples of authentication items include passwords, FORTEZZA cards, and biometrics such as fingerprints, retinal scans, or voice recordings.

d. *Password Management.* The user is responsible for maintaining the security of all passwords. Any password the user is permitted to set should follow these guidelines:
(1) Have at least six characters;
(2) Be a combination of letters and numbers;
(3) Be different than the USERID/identifier;
(4) Never be displayed, shared, or written down;
(5) Not be a word found in a dictionary or otherwise easily guessed (children's names, mother's maiden name, place of birth, etc.);
(6) Not be any of the above spelled backwards or with a digit added;
(7) Not be a string of the same letter or digit;
(8) Be changed at regular intervals, not more than 90 days; and
(9) Never be reused or used on more than one system.

e. *Software Security Procedures.* It is illegal to make or distribute copies of copyrighted material without authorization from the copyright holder. The only exception is the user's right to make a backup copy if the manufacturer does not provide one. Any shareware loaded by the user onto DMS components should not conflict with service-wide software, be approved for use, be scanned for viruses before installation, and should be properly licensed.

f. *Reportable Computer Incidents.* Any suspicious incidents should be immediately reported to a member of the Information Systems Security Team. Reportable incidents include:
- Suspected computer viruses
- Suspected unusual activity
- Evidence of vandalism
- Attempts to bypass access controls
- Unauthorized data alteration
- Denial of service or threats of denial of service attacks
- Unauthorized data disclosure
- Unauthorized data destruction
- Misuse or abuse of computer resources
- Compromise of data via telecommunications
- Loss and/or theft.

Chapter 5 IASO and Other Hierarchies

As the primary site security officer, the IASO will be interacting with members of all three DMS hierarchies. Below are descriptions of the roles of the Certification and Approval Hierarchies.

5-1 Certification Hierarchy

For more information on the Certification Hierarchy, see NSA's NAG 69B Information System Security Policy and Certification Practice Statement for Certification Authorities

a. *Policy Approving Authority (PAA).* NSA serves as the PAA. The PAA is the top level authority of the IAS CMI hierarchy until NSA grants authority for the designation of an Army Policy Creation Authority (PCA).

b. *Policy Creation Authority.* A PCA is the administrative root of a security policy domain of IAS users and other subsidiary authorities. The PCA registers CAs who serve its domain and issues their certificates. A PCA has the capability to issue certificates to users and entities but is not normally expected to do this. A PCA also will issue Certificate Revocation Lists (CRLs) and Compromised Key Lists (CKLs) for its domain. A PCA is the only authority that can issue a CKL.

c. *Army Approving Authority.* USACCSLA serves as the Army Approving Authority, a function similar to a PCA (and is expected to be the PCA for the Army when PCAs are distributed to the S/As).

d. *Certificate Authority (CA).* The CA is responsible for the evaluation of the security features of an information system. The CA reports to the DAA regarding information system security. The CA's other responsibilities include:
- Ensuring the Information Systems Security Policy is implemented,
- Advising the DAA on specific security mechanisms,
- Maintaining accreditation documentation
- Evaluating threats and vulnerabilities,
- Ensuring the Security Testing and Evaluation is completed and documented,

- Maintaining a record of all security vulnerabilities,
- Reporting serious or unresolved violations to DAA,
- Ensuring that each information system is certified,
- Evaluating certification documentation, and
- Ensuring that all ISSMs and IASOs receive appropriate training.

e. *Registration Authority (RA).* USACESO serves as the Army RA. The Army Registration Authority is responsible for developing and defining DMS registration guidance and policy.

f. *Subordinate Registration Authority (SRA).* SRAs implement registration policies and functions at the MACOM level and are the sole source of Army Directory expertise for the site. SRAs develop registration policies and procedures for local registration authorities.

g. *Organizational Registration Authorities (ORA).* This is an optional role and may exist based on site size and volume of registration needs. An Organizational Registration Authority (ORA) assists a CA with registering users by gathering user registration requests and forwarding validated forms to the CA and either to the Sub-Registration Authority (SRA) for entry into the Directory or by entering information into the Directory (if so authorized by an SRA via the registrar). An ORA cannot issue certificates, CKLs or CRLs. An ORA is used to distribute or decentralize part of the administrative tasks of a CA and/or SRA. In the case of large sites, the ORA will be assigned an assistant known as a Sub-Organizational Registration Authority (SORA).

5-2 Approval Roles and Responsibilities

The following paragraphs provide a description of the roles and responsibilities of the DAAs involved in the DMS accreditation process.

a. *Approval Process.* To ensure that the DMS is operating in an acceptable manner, DMS shall be formally accredited by cognizant DAAs issuing an approval to operate. DMS accreditation for the DoD will follow the process described in the DoD Information Technology (IT) Security C&A Process (DITSCAP), 5200.40 (30 December 1997). Accreditation of DMS implementations on SCI networks will be accomplished in accordance with DCID 1/16. Applicable policy statements are:
   (1) The DMS shall be formally approved to operate by the cognizant DAAs.
   (2) Significant changes to approved components, infrastructure, or enclaves will require another formal approval (or reaccredidation).

b. *DMS Designated Approving Authorities.* For the DoD, the DMS DAAs are the Director, NSA; the Director, Defense Intelligence Agency (DIA); the Director, Defense Information Systems Agency (DISA); and the Joint Staff (JS) J6. Collectively, these DAAs are responsible for approving DMS components which satisfy DMS messaging and directory requirements in support of the Military Services and defense and intelligence agencies' implementations. In all cases, each system-level DMS DAA is held to be preeminent in its respective area of responsibility. The DAAs are not responsible for approving specific local implementations of the components by the Military Services and Defense and Intelligence Agencies. Local accreditation of the systems running DMS components is the responsibility of the local DAA consistent with the guidance from the system DAAs. The DMS DAAs address issues affecting the security of the DMS as a system. As necessary, they will designate working groups to address these issues and ensure that overall security of DMS is maintained. When addressing these issues and approving components, the DAAs will base their decisions on a balance of threat, vulnerability, operational requirements, cost, performance, and other significant factors. The DMS DAAs will also ensure that specific implementation security policies that are necessary to execute the policy statements of this document are developed and maintained. The DMS DAAs will ensure this policy document is reviewed periodically and revised as appropriate.
   (1) *NSA DAA*. In addition to being one of four DAAs responsible for the overall security of the DMS, the NSA DAA is responsible for the accreditation of those systems that are running the DMS application that support CRITICOMM messaging, directory, and service management services. The NSA DAA will accredit the SCI Global Operations and Security Center (GOSC) jointly with DIA.
   (2) *DIA DAA.* In addition to being one of four DAAs responsible for the overall security of DMS, the DIA DAA will accredit the SCI GOSC jointly with NSA.
   (3) *DISA DAA.* In addition to being one of four DAAs responsible for the overall security of DMS, the DISA DAA is responsible for accrediting the DMS infrastructure that includes the GENSER (non-SCI, non-Single Integrated Operational Plan) GOSC and all GENSER ROSCs. All GENSER LCCs and systems hosting other GENSER DMS Infrastructure components will be jointly accredited with the local DAA.
   (4) *Joint Staff DAA.* In addition to being one of four DAAs responsible for the overall security of DMS, the JS DAA is responsible for accrediting those systems running the DMS application that handle Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI)

messaging, directory, and management services.

c. *Military Service and Defense Agency DAAs.* Each Military Service and Defense Agency DAA is responsible for accrediting its specific implementation within its local communications enclaves that run the DMS application in accordance with this policy and with its Military Service or Defense Agency security policy. Military Service and Defense Agency DAAs will jointly accredit LCCs within their purview with the cognizant system-level DAA. LCCs and systems hosting DMS infrastructure components are also jointly accredited. Those systems hosting only user components will be under the purview of the cognizant Military Service or Defense Agency DAA. Local DAAs remain responsible for accrediting local GENSER systems, including systems that run the DMS user application.

Chapter 6 DMS Security Mechanisms

6-1 Overview of FORTEZZA

The FORTEZZA card is the basis of DMS system security. The FORTEZZA is a credit-card-sized item that fits into PCMCIA card readers internally or externally attached to trusted workstations. The FORTEZZA is programmed with "personalities" that, when used in combination with a PIN, allow a user to use the workstation.

a. *FORTEZZA Personalities.* The term "personality" refers to a role that a user may serve in an organization or as an individual. A user may have multiple personalities, each of which corresponds to a unique certificate binding the distinguished name, public keys, and clearance/privilege authorizations for that personality. At the time a certificate is loaded on the FORTEZZA card by the CAW, a label is stored with the certificate on the card. This label is known as the "personality label" and is employed by the user to refer to the certificate and private key material to be used when signing and encrypting information. A single FORTEZZA card can hold multiple personalities.

b. *Types of FORTEZZA Card.* FORTEZZA cards can be issued to individual users, organizations, and to DMS components. An individual card is assigned to a specific person and should not be shared with another person. An organizational card represents an organization as opposed to a specific person, and can be used by multiple authorized people. The FORTEZZA card for the SECRET CAW is considered classified material whether or not it is in use. When the SECRET CAW FORTEZZA is not in use it must be stored in the same manner as secret cryptographic materials.

c. *IASO's FORTEZZA Responsibilities.* The IASO is in charge of component FORTEZZA cards. The IASO is also in charge of overseeing the issuance of FORTEZZA cards to users and investigating the loss or destruction of user's cards.

6-2 Generation of FORTEZZA Cards

a. *Card Programming.* Once a user or entity is registered, the CA prepares a user FORTEZZA card if the user is to have access to DMS.

b. *Key Generation.* The CA places a set of public and private key pairs on a FORTEZZA card. One is for confidentiality and the other is for identification and authentication. The CA then assigns a Key Material Identifier (KMID). The KMID is used to identify the relationship between the key pairs. If the private key needs to be designated as compromised on a CKL (an X.509 certificate contains two keys but only one KMID) listing the KMID on the CKL will invalidate both key pairs.

c. *Certificate Generation.* Using information gathered during registration, the CA creates an X.509 certificate. The X.509 certificate will bind the user's public key and authorizations with the user's identity in a trustable association. The complete X.509 certificate is digitally signed with the CA's electronic signature.

d. *Card Management.* Aside from card programming, the CAW application may perform management functions on a FORTEZZA card including the ability to back up and restore a card certificate, delete a certificate, totally restore all the previously resident certificates onto a card, copy an entire card to a new card, zeroize a card, change the PIN, and load a new firmware version into a card.

e. *Card and PIN Distribution.* Once the card has been programmed, it must be distributed to the user or entity securely. Secure distribution ensures that the card was delivered to the user (including obtaining a receipt sent from the user to the CA that the delivery was made), that the card and PIN were delivered separately, and that tampering with the card or PIN did not occur during distribution.

f. *Certificate Revocation.* Authorities who sign certificates also must generate CRLs that list certificates still in their validity interval but that no longer represent a valid binding between a public key and a Distinguished Name (DN) or privilege.

g. *Key and Certificate Compromise.* If a private key is determined to have been (or suspected of having been) compromised, it is the responsibility of the PCA to place the KMID of the compromised key on a CKL. The CKL is then actively distributed from the PCA to the CAs and on to each user throughout the PCA's enclave. Each CA under the PCA must support the PCA both in

providing timely information regarding possible compromises and in actively distributing the CKL delivered by the PCA to their users. The CKL also will be posted to the Directory monthly even if there are no changes.

h. *Audit.* CAW software is designed to automatically record security-related events. The primary purpose of audit in CMI is to detect misuse or incorrect operation of CMI components and to reveal any violations of the stated security policy. Information gathered as part of the audit process will be used to support damage assessments after a security violation. In addition, knowledge that the system's functions and processes are being audited also may act as a deterrent to users behaving in a way that is not consistent with the stated security policy. Review, archive, and deletion of the audit log will be performed by the IASO. The CA shall not be able to read from, write to, or otherwise modify the audit log.

i. *Archive.* Certain data produced by the CMI must be archived to support a number of possible scenarios including database restoration, investigation of possible security compromises, and legal questions related to transaction (e.g., non-repudiation) made involving the CMI components.

j. *Data Recovery.* Data recovery services entail storage of private keys (i.e., for confidentiality) to support recovery of user encrypted data.

6-3 FORTEZZA Security Issues

a. *Overview.* There are two ways in which FORTEZZA security can be breached. The first is for anyone other than the registered user to have access to both the FORTEZZA card and its PIN number. The second is loss of the card itself.

b. *Issuance of Cards.* The IASO and the CA will develop a FORTEZZA issuance policy that will prevent compromise of the cards or PIN numbers.

(1) *Hand Delivery.* The preferred method of issuance is hand delivery of both the FORTEZZA card and PIN. Hand delivery provides the greatest assurance that the proper individual received the card and PIN without complication. For hand delivery, the user must meet with the CA or ORA and provide proper identification.

(2) *Shipping Cards.* If hand delivery is not possible, then the CA or ORA must ship the card and PIN to the user using approved shipping methods (registered mail, etc.). To prevent compromise, the card and PIN must be sent to different addresses using different shipping methods. The user is responsible for acknowledging receipt by signing and returning the included FORTEZZA User Advisory Statement.

c. *Compromise of FORTEZZA Card.* The FORTEZZA card and PIN are to be considered compromised if:

- A shipped card or PIN is not received or
- Someone other than the user has access to both the FORTEZZA card and PIN.

d. *Procedure for Compromised Cards.* If a FORTEZZA card is suspected to be compromised, the card's user is required to immediately notify the site SO. The SO shall then notify the CA. The CA will then list the compromised card in the appropriate CRL and CKL per instructions in NAG 69B.

e. *Emergency Destruction Procedures for FORTEZZA.* Only classified FORTEZZA cards require physical destruction in case of emergency. To prevent a FORTEZZA SECRET card from capture by an unauthorized person, the card must be bent or broken in half. Use a hammer or other heavy object to destroy the card casing.

Chapter 7 Certification and Asset Management

7-1 Overview

NSA has developed a unified Certification Management Infrastructure (CMI) that will provide common security management services required by the FORTEZZA card (and compatible devices) used by IAS components such as workstations, guards, firewalls, routers, and trusted databases and workstations. Specific details of functions, roles, responsibilities and procedures follow. This section establishes the Army CMI security management services, which complement the CMI and which are critical to secure operation of under IAS. This document implements and supplements NSA guidance as defined by NSA's NAG 69B, Information System Security Policy and Certification Practice Statement for Certification Authorities, latest revision. CMI security management services for DMS include controls for:

a. Key Generation, storage, and recovery
b. Rekey
c. FORTEZZA Card (and compatible device) initialization, programming and management
d. Privilege and Authorization Management
e. System Management Functions (e.g., audit, card and certificate tracking, and archive)

7-2 CMI Task Summary

a. *Entity Registration*. The purpose of the registration process is three-fold:

(1) To establish the identity of the entity (individual, object, application)

(2) To validate that the entity has a requirement for a FORTEZZA and X.509 certificate with requested privileges, authorizations, and classification levels.

(3) To gather the forms necessary to build X.509 certificates and to program and distribute FORTEZZA cards and PINs.

b. *Card Programming*. Once a user or entity is registered, the CA prepares a user FORTEZZA card if the user is to have access to DMS.

c. *Key Generation*. The CA places a set of public and private key pairs on a FORTEZZA card. One is for confidentiality and the other is for identification and authentication. The CA then assigns a Key Material Identifier (KMID). The KMID is used to identify the relationship between the key pairs. If the private key needs to be designated as compromised on a CKL (an X.509 certificate contains two keys but only one KMID) listing the KMID on the CKL will invalidate both key pairs.

d. *Certificate Generation*. Using information gathered during registration, the CA creates an X.509 certificate. The X.509 certificate will bind the user's public key and authorizations with the user's identity in a trustable association. The complete X.509 certificate is digitally signed with the CA's electronic signature.

e. *Card Management*. Aside from card programming, the CAW application may perform management functions on a FORTEZZA card including the ability to: back up and restore a card certificate, delete a certificate, totally restore all the previously resident certificates onto a card, copy an entire card to a new card, zeroize a card, change the PIN, and load a new firmware version into a card.

f. *Card and PIN Distribution*. Once the card has been programmed, it must be distributed to the user or entity securely. Secure distribution ensures that the card was delivered to the user (including obtaining a receipt sent from the user to the CA that the delivery was made), that the card and PIN were delivered separately, and that tampering with the card or PIN did not occur during distribution.

g. *Certificate Revocation.* Authorities who sign certificates also must generate CRLs that list certificates still in their validity interval, but that no longer represent a valid binding between a public key and a Distinguished Name (DN) or privilege

h. *Key and Certificate Compromise*. If a private key is determined to have been (or suspected of having been) compromised, it is the responsibility of the PCA to place the KMID of the compromised key on a CKL. The CKL is then actively distributed from the PCA to the CAs and on to each user throughout the PCA's enclave. Each CA under the PCA must support the PCA both in providing timely information regarding possible compromises and in actively distributing the CKL delivered by the PCA to their users. The CKL also will be posted to the Directory monthly even if there are no changes.

i. *Audit*. CAW software is designed to automatically record security-related events. The primary purpose of audit in CMI is to detect misuse or incorrect operation of CMI components and to reveal any violations of the stated security policy. Information gathered as part of the audit process will be used to support damage assessments after a security violation. In addition, knowledge that the systems functions and processes are being audited also may act as a deterrent to users behaving in a way that is not consistent with the stated security policy. Review, archive, and deletion of the audit log will be performed by the IASO. The CA shall not be able to read from, write to, or otherwise modify the audit log.

j. *Archive*. Certain data produced by the CMI must be archived to support a number of possible scenarios including database restoration, investigation of possible security compromises, and legal questions related to transaction (e.g., nonrepudiation) made involving the CMI components.

k. *Data Recovery*. Data recovery services entail storage of private keys (i.e., for confidentiality) to support recovery of user encrypted data.

l. *Other Related Services External to the CMI*. *X.500 Directory*. The Directory contains administrative information (e.g., addresses) and security-related user information (e.g., X.509 certificates, CRLs, and CKLs).

7-3 CMI System Security Requirements

a. *Access Control*. CMI security requirements limit access of each operator only to the information or material needed when performing assigned duties and to the capabilities and access of each element to the information needed to perform assigned functions.

b. *Audit*. CMI personnel shall conduct independent reviews and examinations of system records and operator activities to ensure compliance and to detect noncompliance with established policy and procedures. CMI security procedures shall be used to prevent modification, deletion, or destruction of audit information.

c. *Cryptography*. CMI procedures shall employ principles, means, and methods for rendering security-sensitive information unintelligible to those who do not have access to the information and for restoring encrypted information to an intelligible form for those who do have access to the data.

d. *Tracking and Accounting*. CMI procedures shall ensure that local personnel have the means to determine the status and location of sensitive information and material (e.g., FORTEZZA cards and certificates) that it produces.

e. *Integrity Checks*. CMI procedures shall protect software, hardware, data, keys, and certificates from accidental or malicious alteration.

f. *Protective Technologies*. CMI personnel shall use tamper-evident features and materials developed to detect tampering and to deter attempts to compromise, modify, penetrate, extract, or substitute information processing equipment and cryptographic material (e.g., keys, certificates).

g. *Procedure*. CMI personnel and procedures shall operate consistent with defined policy, doctrine, and operational instructions for the safeguard of requirements and information and for correct operation of the system. The CA shall execute assigned duties in response to a valid user request.

h. *Information Sensitivity*. The private-key component generated and managed by the CMI security system for IAS confidentiality services takes on the classification of the data it is used to protect. All other information generated in the CMI (e.g., CRLs, CKLs, reports, certificates, etc.) is UNCLASSIFIED.

i. *Operating Modes*. CMI procedures shall evolve to achieve a multi-level secure mode of operation.

j. *Physical Interactions*. The hardware (e.g., FORTEZZA cards, platforms, peripherals, network connections) and software (e.g., applications, operating systems) components that constitute the CAW, or interact directly with the CAW workstation shall be approved by NSA.

k. *Personnel Security*. Users with unattended access to an operational CMI component must be of unquestionable loyalty, trustworthiness, and integrity. All personnel who operate as a CA must have a valid security clearance to the level commensurate with the classification of keys and certificates that they issue and consent, if requested, to a nonlifestyle polygraph regardless of the classification of keys and certificates issued.

l. *Personnel Training*. The person selected to perform the CA role must be trained in CAW operation, local DMS configuration, and local security procedures.

m. *Identification and Authentication*. CMI elements and operators shall be uniquely identified and registered in the system. Authentication of such identity is the basis for access to CMI, validating messages, and recording actions of a given element or operator.

n. *System Backups*. CMI elements shall be backed up periodically to maximize system availability and for reconstitution if a human or natural disaster occurs.

o. *CAW Facility*. The correct, secure operation of the CAW is vital to security of the IAS infrastructure. Both CAW hardware and software must be secured and protected from misuse and modification. The CAW's FORTEZZA card and associated PIN shall be protected against unauthorized use.

p. *Separation of Card and PIN*. CMI controls and procedures shall minimize the possibility of someone other than an user gaining access to both the FORTEZZA card and its associated PIN.

q. *Archive*. The CMI shall provide a tamper-proof archive facility to help determine all valid, revoked, and compromised keys from the PAA to users or entities at any given point in time over 30 years.

7-4 Facility Security Criteria

a. The CAW is a dedicated, special-purpose device, and trusted workstation that shall not be used for any purpose it is not designed to perform. As such, physical security controls must be implemented that protect the CAW hardware and software from misuse and modification. In addition, the CA FORTEZZA card and associated PIN must be protected from unauthorized use. Access to the CAW and the CA FORTEZZA card and PIN is limited to personnel who perform one of the CMI roles designated below. Ways to implement this requirement are:
   (1) Controlling access to the room that contains the CAW with an access control list. Anyone not on the access list must be escorted by a person on the list (preferred method).
   (2) Ensuring that the CAW is locked in a secure room or storage area when not in use.

b. The facility must have a place to store any backup and distribution media for the CAW in any manner sufficient to prevent loss, tampering, or unauthorized use of the backup information. Backup tapes and disks must be stored at a site different from where the CAW resides to permit restoration if a natural or manmade disaster occurs at the primary facility. The PCA facility may be used for this service. Data shall be retained in an offsite storage facility for at least 30 years due to legal implications associated with use of digital signatures.

c. Facility security procedures must be in place consistent with the classification level and/or sensitivity of the information being protected. If adequate facility security procedures are not already in place, they must be implemented. (refer to Safeguarding COMSEC Facilities and Material NSTC ISSI 4005 [draft] and AR 380-5).

d. The minimum protection levels to be implemented for the facility in which a CAW is operated are:
   (1) A security check of the facility that houses the CAW shall be made at least once every 24 hours. If the facility is attended continuously, this may be a visual check once each shift to ensure the FORTEZZA card is removed from the CAW and is stored securely when not in use, the CAW is safeguarded, and physical security systems (e.g., door locks, vent covers, etc.) are functioning.
   (2) If the facility is not attended continuously, the security check shall be conducted

before the last person departs from the facility each day. The check shall ensure that the FORTEZZA card is removed from the CAW, that security containers are properly secured, and that the area is secured against unauthorized access. The last person to depart will initial a sign-out sheet that verifies the facility is locked and installed intrusion detection systems are activated.

(3) If the facility is in an area that poses a high risk of unauthorized access and will be unattended for periods longer than 24 hours, it must be protected by an intrusion detection system. A check will be made at least once every 24 hours to ensure all doors to the facility are locked and there were no attempts at forceful entry.

(4) When not in use, the FORTEZZA card used for the Unclassified CAW must be stored in a lockable container sufficient for housing equipment commensurate with the sensitivity level being protected. Access is allowed only to authorized CA operators. The FORTEZZA card used for the SECRET CAW is classified SECRET when not in use. When not in use, it will be stored in a container approved for SECRET cryptographic material storage where access is allowed only to authorized CAW operators.

7-5 Personnel Security Criteria

Traditional UNIX systems rely on one administrator with root privilege. The CAW avoids this weakness by dividing administrative responsibilities into distinct roles. The roles need to support the CAW are the CA, the SA, and the IASO. Wherever possible, separate individuals shall be used to fill each role. If operational circumstances prohibit this, the SA and IASO roles may be combined as long as separate accounts are maintained on the system for each role, but the CA role may not be combined with any of the other CAW roles. Technical and configuration controls for CMI are:

a. *Two-Party Control*. To minimize the risk of any individual gaining access to private key information, Version 3.0 and later versions of the CAW enforce the use of a two-party mechanism for key extraction. The two parties (CA and IASO) must be established and made known to the PCA before establishing the CAW. This is required so the PCA can include this information as part of the CAW configuration file. (refer to Two-Party Key Control in the CAW, 2 November 1995.)

7-6 Procedural Controls

Specific procedural criteria shall be satisfied to ensure that the CMI operates in a secure, trustworthy manner. The functions used to ensure criteria are met are:
Registration.

(1) To prevent unauthorized admission into a domain, a registration process will be used that properly identifies each user and has the security manager verify security information. In addition, each individual has a need to obtain a certificate with a given set of privileges.

(2) Registration may be started by the user who will be registered, by a registration authority or CA, or by another organizational officer who is setting up a local network. The process will ensure that for each type of registration, the user has the proper identification and verification for a card with the requested privileges.

(3) The CA or registration authority will ensure that the user's DN is unique in the system and is appropriate (e.g., matches) for that user. In addition, the clearances and unique DMS messaging privileges will be validated as appropriate for the user by authentication.

a. User-Initiated Registration.

(1) Users approach the security manager first to describe why a card is needed and to present two pieces of identification to verify identity. One of the pieces of identification will be official picture-type identification card such as a driver's license or military or Government civilian identification (e.g., DoD identification card).

(2) If the security manager cannot personally validate that the user requires a card or has all the necessary clearances, the security manager shall consult with the organization's IASO and/or the user's supervisor to validate the requirement.

(3) Registration may be started by the user who will be registered, by a registration authority or CA, or by another organizational officer who is setting up a local network. The process will ensure that for each type of registration, the user has the proper identification and verification for a card with the requested privileges.

(4) The CA or registration authority will ensure that the user's DN is unique in the system and is appropriate (e.g., matches) for that user. In addition, the clearances and unique DMS messaging privileges will be validated as appropriate for the user by authentication.

b. *Security Manager Initiated Registration.* The security manager shall approach the user and validate the user's identify using two pieces of identification to ensure they have the correct individual. One of the pieces of identification will be an official picture-type identification card such as a driver's license or military or Government civilian identification card (e.g., DoD identification

card). The security manager then shall explain that the individual is being processed to receive a FORTEZZA card and require that the candidate complete the X.509 Certificate Request form and DN Request form. The security manager then sends the request to the ORA electronically, by mail, or by hand-delivery. The process is the same as that described above from that point.

c. ORA-Initiated Registration. The ORA shall validate the user's identity as specified above and proceed with established procedures.

7-7 X.509 Certificate and FORTEZZA Card Management.

See DMS Certification Authority Basic Operational Procedures (LOI 25-ca).

7-8 Distribution of FORTEZZA Cards and Personal Identification Numbers

The physical distribution of any FORTEZZA card or PIN introduces the opportunity for compromise. The goal of distribution is to ensure that deliveries are to intended recipients as signified by a receipt, that the card and PIN are delivered separately, and that neither the card nor the PIN were tampered with during distribution. The CA and IASO shall develop a distribution scheme to ensure a continuous chain of events that preclude compromises. Vigorous monitoring and testing of the distribution scheme shall be performed. Delivery methods include:

a. *Unclassified FORTEZZA Cards and PINs.* Hand delivery of the Unclassified FORTEZZA cards and PINs by the CA or ORA when the card is initialized and the PIN is generated is the preferred method of delivery. This requires that the user be present when the card is initialized and the PIN generated. If that is not possible, hand delivery at another location is preferred, but delivery must be by different personnel since the card and PIN cannot be in any individual's possession other than the user, otherwise a compromise has occurred. The user shall be required to provide sufficient identification to the ORA before the card is released. A receipt for the card shall be obtained. Hand delivery provides the greatest assurance that the card was delivered to the proper individual without diversion. When hand delivery is not possible, the cards must be shipped via an approved method, such as registered mail, where there is continuous accountability of the card during distribution, and a signed receipt from the user is generated when the card is delivered. The CA or ORA shall advise the intended recipient of the shipping date, method of shipping, and expected delivery date of the programmed card. In addition to the receipt generated as part of the approved delivery method, users also shall sign and return the FORTEZZA User Advisory Statement (delivered with the card) to the CA, as proof of card receipt and user understanding of responsibilities for use and control of the card. Again, if a PIN is delivered separately from the card, it must be delivered to a separate address (e.g., user's home address) via a different delivery system to ensure that the card and PIN cannot be put together. The CA shall maintain the information to track the card once it is distributed to the user. This information includes the serial number of the card, the name of the individual who has the card, where the person is located, and all the certificates that were programmed on the card. Handling and maintenance of Unclassified FORTEZZA cards will be in accordance with NSA's Operational Security Doctrine for the Sensitive-But-Unclassified (SBU) FORTEZZA Card and Appendix D of this document.

b. *Classified FORTEZZA Cards and PINs.* In accordance with NSA's Operational Policy on the Use of FORTEZZA for Protecting Classified Information, dated 22 January 1996 and Appendix E of this document, FORTEZZA For Classified (FFC) cards will be distributed and tracked via the COMSEC Material Control System (CMCS) as an ALC 4 item (plus serial number tracking). All programmed FFC cards shall be picked up by the local organizational COMSEC Custodian for distribution to users. Delivery from the COMSEC Custodian to the user may occur as described above. Handling and maintenance of SECRET cards will be in accordance with NSA's Operational Security Doctrine for FORTEZZA-For-Classified (FFC) Card and Appendix E of this document.

c. *Distribution of CA Unclassified FORTEZZA Cards.* Initially, a CA's Unclassified FORTEZZA card will be hand carried to each of the initial CAW sites by the team who installs the CAW. The installation team will bring up the CAW using a special test key that was created using a different set of universal keying material than the operational key. CAW operators at the site will be given hands-on training using the CAW test key. When training is complete, an installation team member will load the operational keys and software and hand the operational card to the CA. The CA's PIN letter will be sent to the CA's organizational address via registered mail. The CA must sign for the PIN, then send the receipt back to the PCA.

d. *CA FFC Cards and PINs.* In accordance with NSA's Operational Policy on the Use of FORTEZZA for Protecting Classified Information, dated 22 January 1996, FFC cards for CAs will be distributed and tracked via the CMCS, as an ALC 4 item (plus serial number tracking). FFC Cards will be distributed to users by the organization's COMSEC Custodian. Delivery from the COMSEC Custodian to the user may occur as specified above for user classified FFC cards.

7-9 CMI X.509 Certificate Security Controls

X.509 Certificates contain the private and public keys that enable decryption of messages. Within the CMI are controls by which the X.509 certificates can be controlled if compromised or suspected of compromise. Further detail is provided in LOI 25-ca.

a. *Certificate Revocation List*. A certificate may become invalid and need to be removed from the system via a CRL. A CA places a certificate on a CRL. A certificate will remain on the list until after the inclusion interval. Issuers of certificates will maintain and post their own revocations in the Directory.

b. *CMI Compromise Recovery*. Keys that are compromised are placed on a CKL. Because there is greater potential for attack due to a compromised key, CKLs are actively pushed down the hierarchy starting at the PCA level to each of its CAs, then on to all subordinate CAs, and finally on to the users. CKLs are posted to the Directory also.

7-10 Audit

a. Version 3.0 and later versions of the CAW will audit itself locally. The audit includes:
- Identification and authentication of the CA at FORTEZZA card login
- Input and output from any PCMCIA Interface
- Invocation of cryptographic services
- X.509 certification generation
- Posting of any certificate to the Directory
- Generation or modification of a CRL
- Receipt and distribution of a CRL
- Receipt and distribution of a CKL
- Workstation health check failures
- CAW 3.0 software integrity check for failures.
- Service and device outages (e.g., whether communications lines being unavailable)
- Receipt of improper or misrouted messages
- Modification of the CAW database

b. No CA shall be able to read from, write to, or otherwise modify the audit log.

c. Only the IASO will be allowed to review, delete, and archive the audit log.

d. Deletion of the audit log by the IASO shall only occur after information has been archived.

e. The audit log shall be reviewed at least once each week. Due to the lack of reduction tools in the Version 3.0 CAW and the sheer volume of audit information that may be produced, it may not be practical to review the entire audit log weekly. In that case, a sampling each week of the data must be reviewed to provide a spot check over the CAW operator, and to ensure the CAW is being operated under the security policy.

7-11 Archive

a. As a minimum the CAW shall always archive:
- CRLs and certificates generated at the CAW
- Expired certificates
- Requests to create certificates (including the hard copy user request forms)
- Requests for revocations and compromises
- CKLs received from the PCA
- User FORTEZZA card keying, rekeying, zeroizations, and destruction actions

b. No user shall be able to write to, modify, or delete the archive. However, archived records may be moved to another media if the IASO sees fit.

c. Only authorized users will be allowed to access the archive.

d. The archive records shall be detailed enough to reconstruct the event in terms of time, user making the request, nature of the request, and the results of the action (success or failure).

e. Archive media at the off-site storage location shall be retrievably stored for at least 30 years without any loss of data.

f. All archives must be backed up and stored offsite to ensure the information is available if the primary storage becomes unavailable. The backups will be done at least weekly.

7-12 Information System Security Assistance

Questions or assistance regarding this policy and guidance should be directed through the security chain, the members of which will coordinate any inquiries and assistance with appropriate external ISS elements. IASOs and CAs shall coordinate with NSA's Network Security Management Division about policy and doctrine.

7-13 Asset Security Management

a. *Message Security Overview.* Security management for Army DMS assets (platforms, networks, etc.) involves ensuring the confidentiality of messages; the integrity of messages, nonrepudiation, providing proper access controls and strong unique authentication, and identification. Security of messages transmitted in DMS is ensured by:
- Transmission Security (Encryption Management)
- Access Control Management
- Security Fault Management
- Component Security Certification

b. *User Application.* When a prospective user applies for DMS access, the user or user's supervisor must indicate the security level, security attributes, and precedence level to be authorized. After validation of signatures that ensure the person has access to that ability, the information is entered in the Directory and programmed into the FORTEZZA card. The FORTEZZA card is a primary security factor in DMS. It encrypts the message data and contains the user's certificate and private key. Each certificate must be verified by the UA before a message can be sent. The use of the private key

to encrypt a hash value serves to provide nonrepudiation with proof of the originator's identity.

c. *Security Management.* Security management involves not only ensuring confidentiality of the message, but also protection of the system and network from hostile or inadvertent actions. Security management entails providing a secure system with protective mechanisms (e.g., encryption) to ensure confidentiality, integrity, and a strong identification and authentication process.

d. Transmission Security. Transmission security ensures the security and privacy of message text. Transmission security encrypts the message during transmission, prevents anyone but the intended recipient from reading the message, provides a hashing method of ensuring data integrity, and provides a digital signature to authenticate the originator and to guarantee nonrepudiation of origin.

Chapter 8 Army Information Technology Security Policies, Control Points, and Requirements

8-1 General Security Policy

Any Army IT system that is connected to the DISN, whether or not it is used exclusively for messaging functions, is subject to the provisions of DoD Directive 5200.28, Security Requirements for Automated Information Systems (AISs), and AR 25-IA. This includes DMS components. Each Army IT system or network connected to the DISN must be accredited in accordance with the requirements of the DoD Directive 5200.28; DoD Instruction 5200.40, and as specified in accordance with AR 25-IA. Specific responsibilities are:

a. *U.S. Army as Executive Agent.* PM DMS-A shall function as the executive agent for DMS strategic and tactical portions.

b. *AR 25-IA.* AR *25-IA* implements requirements of DoD Directive 5200.28 and DoD Instruction 5200.40. AR *25-IA* describes and implements necessary requirements, and complies with laws and regulations that govern management, distribution, and protection of Army information.

(1) Capabilities Protection. Data and information channels in the Unclassified domain shall be protected in accordance with NSA Type II requirements. NSA Type I approved mechanisms shall be used in classified domains.

(2) Information Originators. Information originators shall establish the sensitivity of data that reside in their functional area of responsibility.

c. *Record Communication*. AR 25-11, Record Communications and the Privacy Communications System prescribes the policies and responsibilities for the preparation, approval, and processing of record communications within the DA, with an emphasis on the privacy communications system.

8-2 DMS System Security Control Points

a. *Information Protection.* Information in a DMS security boundary shall be implicitly or explicitly identified with protection attributes related to:

- Hierarchical access restrictions
- Categorical access restrictions
- Discretionary access restrictions (owner, group, and/or world)

b. *Access Privileges.* Users of DMS shall be implicitly or explicitly identified with respect to access privileges related to:

- Hierarchical access authorizations
- Categorical access authorizations
- Discretionary access authorizations (owner, group, and/or world)

c. *Separation.* Army personnel shall separate users from data to which they are not privileged or authorized access, under the concept of "least privilege." In other words, users shall not be given access to data for which they do not have the need to know.

d. *Physical Protection.* Army DMS assets shall be physically protected such that security policy is not violated.

e. *Personnel Security.* Personnel security measures shall be established such that user privileges are reliably represented to security policies and procedures that enforce DA's DMS security policy.

f. *Compromise of Information.* Classified and Unclassified information shall not be exposed to compromise.

g. *Unauthorized Data Modification or Corruption.* Data in the system shall be protected from unauthorized modification or corruption.

h. *Unauthorized Asset Modification or Corruption.* Software processes and associated hardware shall be protected from unauthorized modification or corruption.

i. *System Flaws.* Software processes and associated hardware shall be free of flaws that could delay or deny information to authorized users.

j. *User Authenticity.* User authenticity shall be reliably established and represented to all processes acting on behalf of a user.

k. *Information Transfer Protection.* Information units shall be transferred only across paths that reliably enforce the information protection attributes of the transferred information units.

l. *Security Configuration Management.* Army DMS assets shall be protected by a rigorous security Configuration Management (CM) system.

m. *Auditing.* A chronological record of system activities (auditing) shall be implemented at every level throughout the Army as required to ensure traceability. The auditing system shall be sufficient to enable reconstruction, review, and examination of any sequence of events and activities surrounding or leading to an operation, procedure, or event from its inception to final results

n. *Imported Information.* Data imported to the system's security boundary shall be authenticated and reliably labeled with appropriate information protection attributes.

o. *Exported Information.* Data exported from system's security boundary shall be reliably marked with appropriate protection attributes.

p. *System Mitigation.* The system shall mitigate operations, procedures, or events in a transaction based on explicitly defined and carefully controlled conditions. Involved personnel shall ensure that such system capabilities are not disabled.

8-3 System Security Requirements Specifications (SSRS)

a. *System Security Requirements Specification Compliance.* A System Security Requirements Specification shall be developed and updated as required by USACCSLA in compliance with DoD and Army policies about the protection of data. The specification deals with authorizing access to information by a user based on the security clearance or privilege of the user and the sensitivity of the information.

(1) *Level of Protection*. The level of protection for DMS is based on the requirements for simultaneously processing different levels of sensitive classified and Unclassified information with multiple categories on the same DMS platform. (The initial effort was for Unclassified data with one or more categories [i.e., Class B1 - Labeled Security Protection]. It migrated rapidly to SECRET data and Unclassified data with one or more categories [i.e., Class B2 - Structured Protection].) This requires security protection mechanisms in place to support separation and isolation of sensitive data from unauthorized users. In accordance with DoD Directive 5200.28, Enclosure 4, and AR 25-IA, Appendix B, the application of a Class B1 multi-level approach migrating to a Class B2 multi-level approach as specified by DoD Directive 5200.28-STD, Trusted Computer System Evaluation Criteria shall be required to provide the needed protection. Army personnel shall ensure that such requirements are met.

b. *DoD Directives and Army Regulations.* Security policies and specifications resulted from DoD Directive 5200.28, DoD 5200.28-STD, AR 25-11, AR 25-AI, and AR 25-IA-1, Control of Compromising Emanations (U) requirements.

c. *System Security Policy Support.* A system security policy (architectural and detailed) supported by the trusted system shall be maintained at each site using DMS over the life cycle of the system.

d. *Security Clearance or Authorization.* The security clearance or authorization of each Army user shall consist of a hierarchical personnel security clearance or authorization (e.g., UNCLASSIFIED, SECRET, etc.) and a set of nonhierarchical security categories, (e.g., Proprietary, For Official Use Only, Privacy Act, Medical, etc.). AR 380-67, Personnel Security Program provides the detailed personnel security requirements.

e. *Sensitivity Label.*

(1) The sensitivity label of a unit of information shall consist of discretionary and mandatory security attributes.

(2) The discretionary security attributes of the information shall consist of need-to-know access permission assignments (e.g., named people, named groups, or both).

(3) The mandatory security attributes of the information shall consist of both hierarchical classification or authorization levels and nonhierarchical categories.

(4) The trusted system shall operate in the appropriate security mode of operation in accordance with DoDD 5200.28 and AR 25-IA. The appropriate level of trust shall be determined in accordance with DoDD 5200.28, Enclosure 4, and AR 25-AI, Appendix B, and shall be as specified by DoD 5200.28-STD.

8-4 General DMS Security Requirements

a. *General Requirements for Trusted Systems.*

(1) The trusted system consists of the security compliant hardware, firmware, and software.

(2) Each trusted system shall enforce individual accountability through log in procedures, audit of security-relevant events, and resource isolation.

(3) The trusted system shall include security protection mechanisms that prevent:

Unauthorized disclosure (compromise) of classified or Unclassified information

Unauthorized alteration (data integrity) of information processed by the system

Unauthorized alteration (system integrity) of the system

b. *Army Fundamental Security Requirements.* The fundamental security requirements that must be accomplished for DMS are described below and mandated by DoD 5200.28-STD.

(1) *Security Policy.* There shall be an explicit, well-defined security policy or set of rules enforced for DMS.

(2) *Marking.* Access control labels shall be associated with objects or passive entities that contain sensitive information (e.g., records, pages, etc.).

(3) *Identification.* Personnel or active entities must be identified (person, process, device, etc.).

(4) *Accountability.* Audit data shall be selectively retained and protected, so actions that affect security can be traced to a responsible individual.

(5) *Assurance.* DMS contains hardware and software mechanisms that can be independently evaluated and ensures the system enforces the security requirements identified above (Requirements 1 through 4). Army personnel shall ensure that such mechanisms are not disabled.

(6) *Continuous Protection.* Mechanisms that enforce basic security requirements shall be continuously protected against tampering and/or unauthorized changes.

8-5 Minimum Army DMS Security Requirements

The requirements of DoD 5200.28-STD and AR 25-AI that are applicable to Army DMS may be implemented via automated means, manual means, or a combination of the two.

a. *Accountability.* Safeguards shall be in place to ensure that each individual with access to a DMS platform is held accountable for any actions taken and that an audit trail is implemented with a documented history of all events. The audit trail shall be of sufficient detail to reconstruct events in order to determine the cause or magnitude of compromise if a security violation or malfunction occurs. Embedded mechanisms shall be set to alarm and report whenever unauthorized events or those that have security implications occur. Audits shall be conducted at least once a week. Audit records shall be retained as directed by the DAA for a period of not less than one year.

b. *Access.* DMS platforms shall be operated under an access control policy. Access to the system shall be controlled by identification and authentication, which will positively establish the identity of each user before granting access. The procedure shall ensure that the user who requests access has the required security clearance or authorization and need-to-know for the information or action requested before admitting the user to the system. Each user shall have a PIN and password assigned before being granted access to the system. Access procedures shall:

(1) *PIN.* PINs shall be generated and issued as specified in DMS Certificate Management Infrastructure (CMI) guidance and shall be delivered separately from password issuance.

(2) *Password.* Passwords shall be controlled by the IASO. Passwords shall be randomly generated by password generating software and shall be stored in encrypted form on the system in a way that is accessible only by the IASO or a designated alternate.

(3) Logon. After a successful logon has been achieved, the system shall display a banner message to notify the user that the system is restricted to authorized use, constitutes consent to monitoring, and is subject to Title 18, U.S. Code, Section 1030, as well as state criminal and civil laws.

(4) *Timeout*. The system shall minimize the amount of information and the usefulness of the data being displayed. A time-out mechanism shall be activated on the system after a pre-determined period of time (maximum 15 minutes inactivity).

(5) *Lockout.* After a specified number of attempts to logon (maximum of three consecutive attempts per user session) by the user, the system shall activate a lock-out mechanism. A report of the incident shall be produced automatically and forwarded to alert the IASO of possible illegal activity.

(6) *Log out.* The system shall automatically log out a user terminal, clearing the terminal screen and closing the connection after a pre-determined period of time (maximum 15 minutes of).

(7) *Permissions.* The concept of "least privilege" shall be enforced (i.e., users may access all the data to which they are entitled, but no more.)

8-6 DMS Administrative Requirements

a. *Security Training and Awareness.* All Army DMS users who access the system shall be trained and made aware of the importance of maintaining system security as well as the mechanisms and procedures required to maintain proper ISS posture. Training shall be formally documented along with other required security briefings.

b. *Contingency Plan.* A contingency plan in accordance with Installation Information Services, DA PAM 25-1-1 shall be developed so that if data is modified or destroyed unexpectedly, recovery procedures are available.

c. *Security Concept of Operations.* A security concept of operations (CONOPS) shall be developed for each DMS installation. The CONOPS shall describe how to securely operate and maintain DMS components.

d. *System Sensitivity Designation.* Data shall not be introduced into a DMS component without the originator designating its classification and sensitivity.

e. *Security Mode of Operation.* The security processing mode of operation will be determined based on the highest classification and formal categories of data, clearance, access approval, and need-to-know of system users.

f. *Classification Guide.* A classification guide shall be issued that provides classification guidance for locally managed DMS assets.

g. *Operations Security.* Army MACOMS, PM DMS Army (DMS-A), and DISC4 will address Operations Security (OPSEC) in accordance with Operations Security (OPSEC), AR 530-1 to protect information.

h. *Threat Assessment Intelligence Support.* Early and continued collaboration among the intelligence, security engineering, requirements generation, developers, PMs, and other affected DMS elements shall be maintained to ensure timely availability of threat information. Accomplishment of system threat assessments shall address:

(1) Key intelligence judgements and significant changes in the threat environment.

(2) Developmental and operational threat environments, the threats to be countered, system specific threats, reactive threats, and technologically feasible threats should form the core of the assessment.

(3) The status of critical intelligence categories. Intelligence production requirements that support these categories shall be identified early for inclusion in program plans and costs estimates.

i. *Compromising Emanations.* Army MACOMS, PM DMS-A, and DISC4 will address the AR 25-AI-1 TEMPEST control requirements.

j. *Security Plan.* The DMS is an AIS. In accordance with AR 25-AI, Paragraph 2-3a(12), a generic security plan shall be developed and maintained for the life of the system. After transition from PM control to operational control, the maintenance of the security plan shall be the responsibility of the using MACOM.

k. *Certification and Accreditation.* Each DMS site and every individual involved in DMS operations shall support DoD Instruction 5200.40 requirements under the DoD Information Technology System Certification and Accreditation Program (DITSCAP) and Information Technology Management Reform Act (ITMRA) when requested to do so by the DAA, a DMS manager, or any representative of a local Security organization.

8-7 Automated Information System Security Procedural Requirements

There are a significant number of procedural requirements that result from implementation of an AIS the size and complexity of DMS. Most requirements are not DMS specific; however, they are applicable to DMS.

a. *Reporting and Accountability*. Reporting and accountability procedures for locally managed DMS assets shall be implemented at each DMS site.

b. *Password Management.* A password management system shall be implemented to control generating, issuing, distributing, and storing passwords.

c. *Media Protection.* Procedures shall be established to protect classified media. Protection of Unclassified data shall be in accordance with applicable directives and regulations.

d. *Network Security.* Network security on locally managed networks shall ensure that confidentiality, integrity, authentication, nonrepudiation, guaranteed and timely delivery, inter-operability and survivability are adequately addressed.

e. *Physical Security.* Locally managed DMS assets shall have physical controls commensurate with the information contained in the system.

f. *Security Management.* At each DMS site, a local security management system shall be developed in which security functions, mechanisms, and services are developed and used to achieve message and system accountability, confidentiality, integrity, and access control. Such a system shall include local management requirements as well as requirements of the CMI system.

g. *Software.* Safeguards shall be implemented in all software used in conjunction with DMS that will protect against both compromise and unauthorized manipulation.

h. *Viruses.* All DMS sites will take appropriate action to install virus protection software and procedures that are required to protect against infection and spread of malicious code.

i. *Hardware.* To the maximum extent possible, cost-effective hardware security procedures shall be implemented for DMS components.

j. *Life-Cycle Maintenance.* Maintenance controls shall be implemented for Army DMS components.

k. *Personnel Security.* Personnel who manage, design, develop, maintain, or operate local DMS assets shall undergo initial and periodic security awareness training.

l. *Remote Devices.* Remote devices shall be secured consistent with the mode of operation and data that the remote device is authorized to access.

8-8 Data Integrity

Access and audit safeguards shall be implemented and shall be of sufficient strength to detect and minimize inadvertent modification or destruction of data and to detect and prevent malicious data modification or destruction.

8-9 Data Continuity

Each file or record in DMS shall have an identifiable source or proponent throughout its life. Accessibility, maintenance, movement, and disposition shall be governed by security clearance or authorization, formal access approval, and need-to-know as appropriate.

8-10 Continuous Protection

Each trusted system shall be self-protecting to prevent unauthorized on-line changes. All changes to the trusted system and attempts to change the trusted system shall be audited.

8-11 Additional Security Requirements

DMS shall include data processing capabilities for protecting information processed and managed by the system. This includes parts of the operating system and the applications software as well as hardware and firmware that provide for the security protection specified. The local DMS components shall enforce the security requirements specified below.

a. *Identification of Subjects and Objects.* The detailed security requirements for the trusted system are described in terms of subjects and objects and the interaction between them. This involves mapping named resources of the system into two categories and defining the relationships between the categories.

b. *Definition and Concepts.* The terms 'subject' and 'object' are introduced to define some of the detailed security requirements for DMS. The properties of and relationships between these entities are:

(1) *Subject.* A subject is an active entity that can cause information to flow among objects or change the system state. It can take the form of a device, a program that is being operated (i.e., a process), or a generic user (any person working at a DMS terminal or an external system connected to the system, such that associated activities are architecturally viewed as occurring at an operational terminal).

(2) *Object.* An object is a passive entity that contains information. Access to an object implies access to contained information. Objects can be hardware resources or software creations; physical resources or logical abstractions; permanent or temporary; or Unclassified or classified.

(3) *Object Sensitivity Level Categories.* Object sensitivity use can be categorized into two types: single-level and multi-level. The distinction is based on mandatory security attributes.

(a) A single-level object can only be assigned one sensitivity label at any time, but the assignment can be changed while the system is operating.

(b) A multi-level object can simultaneously hold data objects with different sensitivity levels.

c. *Identification Requirements.*

(1) Named resources accessible to DMS shall be mapped into subjects and objects.

(2) Every subject or object under DMS control shall be provided with a unique identifier.

(3) For every subject, DMS shall be able to determine its type (e.g., SA, IASO, user) and applicable security access characteristics (i.e., mandatory or discretionary).

(4) (Only registered subjects shall be permitted access to objects. Every attempt by a subject to access a named object shall be controlled by DMS. The access shall be permitted only when the subject's security characteristics are compatible with the object's according to specified security rules.

8-12 Labels

Local DMS systems shall preserve sensitivity labels associated with each subject and storage object under their control. In addition, the local systems shall ensure sensitivity labels accurately represent the sensitivity level of specific subjects and objects. When exported by DMS, sensitivity labels shall accurately, unambiguously represent the internal labels and shall be associated with the information to be exported. To import unlabeled data, the local DMS system shall request and receive the security level of data from an authorized user. The information labels shall be the basis for access control. Sensitivity requirements, as applied to subjects and objects, include a number of restrictors. Local DMS personnel are responsible for ensuring that labels are protected in their domains. There are levels of security access (e.g., Unclassified, TOP SECRET, SECRET, SPECIAL ACCESS REQUIRED, and special compartments). These access levels make up a hierarchical structure based on the actual levels of security clearance from TOP SECRET down through UNCLASSIFIED. A nonhierarchical set of distinctions (e.g., Proprietary, Acquisition Sensitive, For Official Use Only, Privacy Act, Medical, etc.) also exists, which comprise restrictors for information. The restrictors establish which individuals or groups are permitted to access information. In addition, the restrictors can be used to limit the type of access permitted to an object. With regard to DMS:

a. DMS personnel shall ensure that sensitive data assigned to each subject and object is retained and is correctly, reliably labeled.

b. DMS personnel shall ensure that sensitive data, associations with the subjects and objects, and data content of the objects are not altered, deleted, or created without proper authorization.

c. DMS personnel shall ensure the protection of multiple sensitivity levels.

d. DMS personnel shall protect the integrity of multiple sensitivity categories.

e. DMS personnel shall ensure that individuals or groups to be included on the discretionary restrictor or access restrictor list are included and allowed access to information specified for their level of access.

8-13 DoD Detailed Specifications

The detailed specifications that follow were derived from DoD 5200.28-STD and are clearly identified in each specification as to the level of trust (Class C2, B1, and B2) for each specific requirement.

a. *Discretionary Access Controls.* The discretionary access control rules define the conditions in DMS under which subjects are allowed to access objects and are intended to prevent compromise of information contained. The access control mechanisms are considered critical in preserving the security provided by DMS. Access to objects by subjects shall be mediated by a discretionary access control mechanism in DMS.

CLASS	REQUIREMENT
C2	Define access between named users and named objects (e.g., files and programs)
C2	Control access between named users and named objects (e.g., files and programs)
C2	Allow users to specify sharing of objects by named individuals, defined groups of individuals, or both
C2	Allow users to control sharing of those objects by named individuals, defined groups of individuals, or both
C2	Provide controls to limit propagation of access rights
C2	By either explicit user action or default, provide that objects are protected from unauthorized access
C2	Be capable of either including or excluding access to the granularity of a single user
C2	Access permission to an object by users not already possessing access permission shall only be assigned by authorized users

b. Object Reuse. Whenever an object used for data storage is initially assigned, allocated, or reallocated to a subject from the DMS pool of unused objects, DMS personnel shall ensure that the object contains only data for which the subject is authorized.

CLASS	REQUIREMENT
C2	Authorizations to information contained in a storage object shall be revoked before initial assignment
C2	Authorizations to information contained in a storage object shall be revoked before allocation to a subject from DMS's pool of unused storage objects
C2	Authorizations to the information contained in a storage object shall be revoked before reallocation to a subject from DMS's pool of unused storage objects
C2	No information, including encrypted representations of information, produced by a prior subject's actions shall be available to any subject that obtains access to an object that has been released back to the system

c. Labels.

CLASS	REQUIREMENT
B2	Sensitivity labels associated with each system resource (e.g., subject, storage object), that is directly accessible by subjects external to DMS shall be maintained by DMS personnel
B2	Sensitivity labels associated with each system resource (e.g., subject, storage object), that is indirectly accessible by subjects external to DMS shall be maintained by DMS personnel
B1	Sensitivity labels shall be used as the basis for mandatory access control decisions
B1	In order to import unlabeled data, DMS personnel shall request and receive the sensitivity level of the data from authorized users
B1	Unlabeled imported data shall be auditable by DMS personnel

d. Label Integrity.

CLASS	REQUIREMENT
B1	Sensitivity labels shall accurately represent security levels of the specific subjects or objects with which they are associated
B1	When exported by DMS, DMS personnel shall ensure sensitivity labels accurately and unambiguously represent the internal labels and are associated with the information being exported

e. Exportation of Labeled Information.

CLASS	REQUIREMENT
B1	DMS personnel shall designate each communication channel and Input or Output (I/O) device as either single level or multi-level
B1	Any change in these label designations shall be done manually and shall be auditable by DMS personnel
B1	DMS personnel shall maintain and be able to audit any change in the sensitivity level or levels associated with a communication or I/O device

f. Exportation to Multi-level Devices.

CLASS	REQUIREMENT
B1	When DMS exports an object to a multi-level I/O device, the sensitivity label associated with that object shall also be exported
B1	The object shall reside on the same physical medium as the exported information
B1	The object shall be in the same form (i.e., machine-readable or human-readable form)
B1	When DMS imports or exports an object over a multi-level communication channel, the protocol on that channel shall provide for unambiguous pairing between the sensitivity labels and the associated information being sent or received

g. Exportation to Single-Level Devices.

CLASS	REQUIREMENT
B1	Single-level I/O devices and single-level communication channels are not required to maintain the sensitivity labels of the information they process
B1	DMS shall include a mechanism by which DMS personnel can reliably communicate to designate the single security level of information imported or exported via that single level communication channel or I/O device

h. Labeling Human-Readable Output.

CLASS	REQUIREMENT
B1	The IASO shall be able to specify the printable label names associated with the exported sensitivity labels
B1	DMS shall mark the beginning and end of all human-readable, paged, hard-copy output that properly represents the sensitivity of the output or that properly represents the sensitivity of the information on the page
B1	DMS shall, by default, mark the top and bottom of each page of human-readable, paged, hard-copy output (e.g., line printer output) with human-readable sensitivity labels that properly represent the overall sensitivity of the output or that properly represent the sensitivity of the information on the page
B1	Any override of these marking defaults shall be auditable by the trusted system
B1	The hierarchical classification or authorization component in human-readable sensitivity labels shall be equal to the greatest hierarchical classification authorization of any of the information in the output that the labels refer to; the nonhierarchical category component shall include all of the nonhierarchical categories of the information in the output the labels refer to, but no other nonhierarchical categories

i. Subject Sensitivity Labels (Changes).

CLASS	REQUIREMENT
B2	DMS shall immediately notify a user of each change in the security level associated with that user during a session
B2	A user shall be able to query the UA as desired for a display of the subject's complete sensitivity label

j. Device Labels.

CLASS	REQUIREMENT
B2	DMS shall support the assignment of minimum security levels to all attached physical devices
B2	DMS shall support the assignment of maximum security levels to all attached physical devices
B2	These security levels shall be used by DMS to enforce constraints imposed by the physical environments in which the devices are located

k. *Mandatory Access Control.* Security policies defined for systems that are used to process classified or other specifically categorized sensitive information must include provisions for enforcement of mandatory access control rules. The mandatory access rules define access based on a comparison of the individual's clearance or authorization and the classification designation of the information being sought.

CLASS	REQUIREMENT
B2	DMS personnel shall enforce a mandatory access control policy over all resources (i.e., subjects, storage objects, and I/O devices) that are directly accessible by subjects external to DMS
B2	DMS personnel shall enforce a mandatory access control policy over resources (i.e., subjects, storage objects, and I/O devices) that are indirectly accessible by subjects external to DMS
B2	These subjects and objects shall be assigned sensitivity labels that are a combination of hierarchical classification levels and nonhierarchical categories, and the labels shall be used as the basis for mandatory access control decisions
B1	DMS shall be able to support two or more such sensitivity levels
B2	DMS requirements shall hold for accesses between subjects external to DMS and objects directly or indirectly accessible
B1	A user can access an object only if the hierarchical classification in the user's sensitivity level is greater than or equal to the hierarchical classification in the object's sensitivity level and the nonhierarchical categories in the user's sensitivity level include the nonhierarchical categories in the object's sensitivity level
B1	A user can write an object only if the hierarchical classification in the user's sensitivity level is less than or equal to the hierarchical classification in the object's sensitivity level and the nonhierarchical categories in the user's sensitivity level include all the nonhierarchical categories in the object's sensitivity level

l. Accountability – Identification and Authentication.

CLASS	REQUIREMENT
C2	DMS shall authenticate the identity of every user. Groups shall be allowed, provided the group is a collection of uniquely identified individuals
B1	The authentication data of each user shall include the unique identity of the user (e.g., PIN, and user name) as well as information for determining the authorizations of individual users
B1	Data shall be used by DMS to authenticate the user's identity and to ensure that the sensitivity level & authorizations of subjects external to DMS that may be created to act on behalf of a user are dominated by the authorization of that user
C2	Authentication data shall be protected so that it cannot be accessed by an unauthorized user
C2	DMS shall be able to enforce individual accountability using the unique identification of each user
C2	DMS shall provide the capability of associating this identity with all auditable actions taken by that individual

m. Trusted Path.

CLASS	REQUIREMENT
B2	DMS shall support a trusted communication path between itself and users used when a trusted system-to-user connection is required (e.g., login, change subject sensitivity level, etc.)
B2	Communications via this trusted path shall be initiated exclusively by a user
B2	Each trusted path shall be logically isolated and unmistakably distinguishable from other paths

n. Audit.

CLASS	REQUIREMENT
B1	DMS shall be able to audit any override of human-readable output markings
B1	For events that introduce an object into a user's address space, the audit record shall include the name of the object and the objects sensitivity level
B1	For object deletion events, the audit record shall include the name of the object and object's sensitivity level
B1	The SA and IASO shall be able to selectively audit the actions of any one or more users based on individual identity and/or object sensitivity level
B2	DMS shall be able to audit the identified events that may be used in the exploitation of covert storage channels
C2	DMS shall be able to create an audit trail of accesses to the objects it protects
C2	DMS shall be able to maintain an audit trail of accesses to the objects it protects
C2	DMS shall be able to protect from modification an audit trail of access to the objects it protects
C2	DMS shall be able to protect from unauthorized access an audit trail of access to the objects it protects
C2	DMS shall be able to protect from destruction an audit trail of access to the objects it protects
C2	The audit data shall be protected by DMS so that read access to it is limited to those who are authorized for audit data
C2	DMS shall be able to record the use of identification mechanisms
C2	DMS shall be able to record the use of authentication mechanisms
C2	DMS shall be able to record the introduction of objects into a user's address space (e.g., file open, program initiation)
C2	DMS shall be able to record the deletion of objects
C2	DMS shall be able to record the actions taken by users
C2	DMS shall be able to record the actions taken by SAs
C2	DMS shall be able to record the actions taken by IASOs
C2	DMS shall be able to record other security relevant events
C2	For each recorded event, the audit record shall identify the date and time of the event
C2	For each recorded event, the audit record shall identify the user
C2	For each recorded event, the audit record shall identify the type of event
C2	For each recorded event, the audit record shall identify the success or failure of the event
C2	For identification/authentication events, the origin of request (e.g., terminal identifier) shall be included in the audit record
C2	DMS shall be able to record all system faults and restart
C2	DMS shall be able to record all diagnostically detected errors

o. Operational Assurance - System Architecture.

CLASS	REQUIREMENT
C2 & B2	DMS shall maintain a domain for its own execution that protects it from external interference (e.g., modification of its code or data structures)
B1	DMS shall maintain process isolation through the provision of distinct address spaces under its control
C2	DMS shall isolate the resources to be protected so that they are subject to the access control and auditing requirements
B2	DMS shall be internally structured into well-defined, largely independent modules
B2	DMS shall make effective use of available hardware to separate those elements that are protection-critical from those that are not
B2	DMS modules shall be designed such that the principle of least privilege is enforced
B2	Features in hardware, such as segmentation, shall be used to support logically distinct storage objects with separate attributes (namely: readable, writable)
B2	The user interface to DMS shall be completely defined and all elements of DMS identified

p. Operational Assurance - System Integrity.

CLASS	REQUIREMENT
C2	Hardware or software diagnostic features shall be provided to periodically validate the correct operation of the on-site hardware and firmware elements of the trusted system. These features shall be controllable by the IASO or a designated alternate
C2	The security policy enforced by DMS shall not be relaxed while on-line diagnostic functions are being executed nor during any degraded conditions detected by the diagnostics functions
B2	The diagnostic features shall not interfere with other DMS functions; if any interference with trusted system functions occur, system operations shall be halted

q. Covert Channel Analysis.

CLASS	REQUIREMENT
B2	The system developer shall have conducted a thorough search for covert storage channels and make a determination (either by actual measurement or by engineering estimation) of the maximum bandwidth of each identified channel

r. Trusted Facility Management.

CLASS	REQUIREMENT
B2	The trusted system shall support separate operator and administrator functions

s. Life Cycle Security Testing.

CLASS	REQUIREMENT
C2	The security mechanisms shall be tested and found to work as claimed in the system documentation
C2	Testing shall be performed to ensure that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the security protection mechanisms
C2	Testing shall include a search for obvious flaws that would allow violation of resource isolation or that would permit unauthorized access to the audit or authentication data
B1	Testing of a trusted system shall subject its design documents, source code, and object code to a thorough analysis test
B1	Testing shall include a search to uncover design and implementation flaws that would permit a subject, external to DMS to read, change, or delete data normally denied under the mandatory or discretionary security policy enforced for DMS
B1	Testing shall ensure that no subject (without authorization to do so) is able to cause the trusted system to enter a state such that it is unable to respond to communications initiated by other users
B1	All discovered flaws shall be corrected and DMS retested to demonstrate that the flaws were eliminated and new flaws were not introduced
B2	DMS shall be tested and found relatively resistant to penetration
B2	Testing shall demonstrate that DMS implementation is consistent with the descriptive top-level specification

t. Life-Cycle Design Specification and Verification.

CLASS	REQUIREMENT
B2	A formal model of the security policy, supported by DMS, shall be maintained over the life cycle of DMS that proves consistent with its axioms
B2	A descriptive top-level specification of DMS shall be maintained that completely and accurately describes DMS in terms of exceptions, error messages, and effects
B2	The descriptive top-level specification shall be shown to be an accurate description of the DMS interface

u. Life-Cycle Configuration Management.

CLASS	REQUIREMENT
B2	During development and maintenance of DMS, a CM system shall be in place that controls changes to the descriptive top-level specification, design data, implementation documents, source code, the running version of the object code, and test fixtures and documentation
B2	The CM system shall ensure a consistent mapping among all documentation and code associated with the current version
B2	Tools shall be provided for generation of a new version of DMS from source code
B2	Tools shall be provided for comparing a newly generated version with the previous version; ascertaining that only intended changes were made that will be used as the new version

v. Security Features User's Guide.

CLASS	REQUIREMENT
C2	A single summary, chapter, or manual in user documentation shall describe the protection mechanisms of DMS, guidelines regarding use and how the mechanisms interact with one another

w. Trusted Facility Manual.

CLASS	REQUIREMENT
C2	A manual addressed to the SA shall present cautions about functions and privileges that should be controlled when running a security facility
C2	The manual shall describe the procedures for examining and maintaining the audit files as well as the detailed record structure for each type of audit event shall be given
B1	The manual shall describe the operator and administrator functions related to security to include changing the security characteristics of a user
B1	The manual shall provide guidelines on the consistent and effective use of the protection features of the system; how the protection features interact; and DMS system and facility procedures, warnings, and privileges that need to be controlled in order to operate the facility in a secure manner
B2	The manual shall identify DMS modules that contain the reference validation mechanism
B2	The manual shall describe the procedures for the secure generation of any new DMS modules or files from the source after modification of any modules in DMS

x. Test Documentation.

CLASS	REQUIREMENT
C2	A document shall be developed that describes the test plan
C2	Test procedures shall be developed that show how the security mechanisms were tested
C2	The results of the security mechanism's functional testing shall be developed also
B2	The results of testing the effectiveness of the methods used to reduce covert channel bandwidths shall be documented

y. Design Documentation.

CLASS	REQUIREMENT
C2	Documentation shall be available that provides a description of the manufacturer's philosophy of protection
C2	Documentation shall be available that provides an explanation of how the philosophy of protection is translated into DMS
C2	Documentation shall describe the interfaces

	between modules
B1	Documentation shall identify the specific protection mechanisms and show how the mechanisms satisfy the security policy model
B2	Documentation shall describe a formal policy model that is proven sufficient and enforced by the system
B2	A descriptive top-level specification shall be prepared and shown to be an accurate description of DMS
B2	The documentation shall describe how DMS implements the reference monitor concept
B2	The documentation shall give an explanation of how the reference monitor is tamper-resistant
B2	The documentation shall explain how the reference monitor cannot be bypassed
B2	The documentation shall explain how the reference monitor is correctly implemented
B2	The documentation shall describe how the

	trusted system is structured to facilitate testing
B2	The documentation shall describe how the trusted system will enforce least privilege
B2	The documentation shall present the results of the covert channel analysis and tradeoffs involved in restricting channels
B2	Auditable events that may be used in the exploitation of known covert storage channels shall be identified and documented
B2	The bandwidths of known covert storage channels, the use of which is not detectable by the auditing mechanisms, shall be provided

Chapter 9 Mobility And Security Issues

9-1 Change to DMS Components

Any change to a site's DMS setup (including but not limited to software, hardware, or component interfaces) shall be reported to the IASO. The IASO must determine the implications of the change to system security. Facility changes may require a Facility TEMPEST Assessment and Risk Analysis in accordance with AR 25-IA.

9-2 Remote or Portable Information Technology Systems

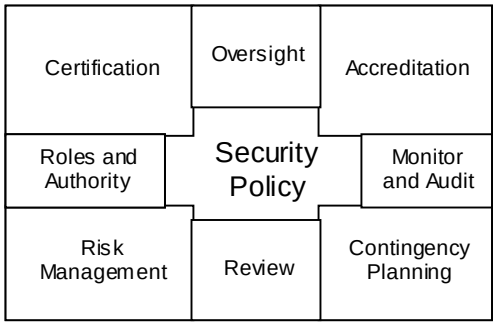
Remote DMS components linked to larger DMS sites, laptops, notebook computers, and any other portable IT system used in DMS deployment shall be certified and accredited for use per AR 25-IA. Any remote or portable component shall be secured in accordance with the highest classification level of data accessed by that component.

9-3 Temporary Duty

A DMS user who needs access to DMS while on Temporary Duty (TDY) must advise the site SO, who shall determine whether the user should be issued a temporary FORTEZZA card or have a new personality programmed onto the user's current card. The new personality shall have an expiration date that covers the length of the TDY assignment. When the user leaves the TDY location, the temporary card will be deactivated and/or the temporary personality will be removed and de-registered. The SOs of the user's current and TDY sites are both responsible for coordinating this assignation, tracking, and de-registration.

Chapter 10 Setting a Security Policy

This section discusses the general requirements for a site security policy for DMS. In the event of conflicting Army policies, the more stringent requirement(s) will take precedence. When the most stringent policy cannot be determined, Major Army Commands will submit a request for a policy decision to the Office of the Director of Information Systems for Command, Control, Communications, and Computers (DISC4).



10-1 Overview of Policy Requirements

A comprehensive security policy begins with an assessment of the value of the DMS data, equipment, and assets. It then discusses how to best protect these assets and assigns responsibility for this protection. Training will be provided so that the affected personnel will understand their responsibilities. Once these ground rules are established, the security policy will explain the

process for monitoring security and assessing the system, including contingency plans and penalties for non-compliance. A good security policy has these attributes:

- It is implementable.
- It is enforceable through security tools.
- It is clear and understandable.
- It is comprehensive.
- It is practical.
- It is cost effective.
- It complies with appropriate laws and regulations.
- It reduces risk.
- It ensures continued availability of operations.
- It ensures confidentiality and integrity of DMS data.

Chapter 11 Security Training

11-1 Security Training for the IASO

All IASOs must complete an Information Assurance security course equal to their assigned duties, including at least one of these four courses:

- Information Assurance System Security Officer's course
- Operational Information System Security CD ROM volumes 1 & 2
- DISC4-sponsored ISS Managers courses
- Equivalent courses as designed by DISC4.

11-2 Security Training for Users

Training is an integral part of DMS Security. All personnel shall be trained to use DMS and its security features and complete an annual security awareness class.

a. *Training Basics.* This training will, at a minimum, cover these subjects:
   - DMS security threats, vulnerabilities, and risks;
   - DMS security services, policies, and regulations; and
   - DMS security-related operational procedures.

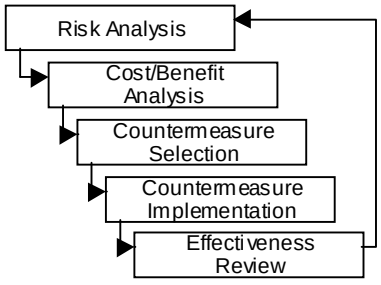
b. *Refresher Training.* Refresher training will be provided annually, and also when:
   - Personnel assume new or different duty responsibilities,
   - Significant changes to DMS are reflected in changed security policies, and
   - New threats to DMS are identified.

c. *Training Formats.* Training can take a variety of formats. Formal classroom training should be used to address specific issues to selected users, such as explaining basic security or projected computer upgrades. Mass Media training via emails, web pages, posters, tapes, films, or newsletters can be used to train step-by-step instructions, legal responsibilities, prevention tips, and other simple data. Because this form of training can be overlooked, a process should be developed for viewers to verify that they have actually read the material. More information on training can be found in Appendix E, DMS Security Awareness and Training draft 2.1.

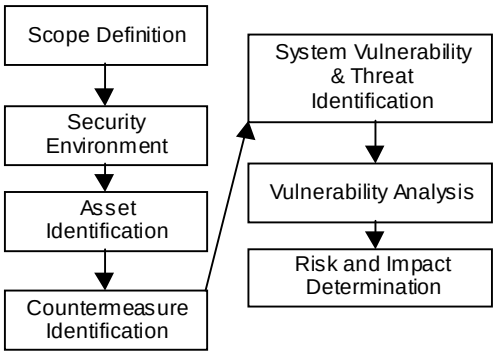
Chapter 12 Assessing and Responding to Threats

12-1 Risk Management

A Risk Assessment is a three-step process wherein threats to system security are identified, the system's vulnerability to the threats is determined, and countermeasures to any vulnerability are devised. Subsidiary concerns are the costs and benefits of changes, countermeasures to threats, and the effectiveness of these countermeasures.



a. *Risk Assessment.* The ISSM and IASO will conduct new risk assessments every 3 years or upon significant changes in the IS environment (including but not limited to system upgrades and component modification.) The findings of the Risk Assessment report shall be safeguarded. Only the DAA, CISSM, or ISSM have permission to disseminate the Risk Assessment report. Unauthorized dissemination is a security violation



b. *Cost/Benefit Analysis.* The Cost/Benefit Analysis weighs the availability of countermeasures against the return on investment and the level of risk. The means of making this decision are outlined below.

c. *Countermeasures.* All countermeasures determined upon should do one or more of the following:
- Prevent threats
- Detect threats
- Correct threats
- Reduce risk
- Prevent loss
- Limit loss
- Transfer loss.

Countermeasures can be administrative, physical, or technical. To determine which countermeasure to use, assess the following considerations:
- How valuable is the information and what would be the risks of losing it?
- Is the level of risk considered acceptable?
- Are there vulnerabilities which are not eliminated?
- Would this countermeasure be cost-effective and give a good return on investment?

If the questions above are answered acceptably, the appropriate manager should:
- Allocate the necessary funds,
- Oversee the implementation of the countermeasure,
- Document the decision, and
- Oversee any necessary changes in site processes, functions, and responsibilities.

d. *Effectiveness Review.* The risk management process should be applied throughout the system life-cycle. Periodic effectiveness reviews should be made after changes to the system or its environment.

12-2 Vulnerability Analysis Assessment Program

The VAAP was developed to identify and mitigate vulnerabilities within networks.

12-3 Information Assurance Vulnerability Alert (IAVA)

IAVAs are a DoD-wide effort to identify and repair security breaches in DISA systems. All IAVA alerts must be responded to, even if the alert is not connected to a system on-site. IAVA alerts contain not only the data on the security breach, but the patch that will prevent further occurrences of the problem.

12-4 Types of Attack

a. *Intruder.* Follow the steps below to determine if your system has been compromised by an intruder.
(1) Examine log files for connections from unusual locations or other unexpected activity.
(2) Look for unexplained setuid or setgidfiles.
(3) Check system binaries for unauthorized alteration.
(4) Check systems for unauthorized packet-sniffing programs.
(5) Examine “cron” and “at” files.
(6) Check for unauthorized modifications to the password file.
(7) Check the system for hidden files.
(8) Check all computers attached to a network. If one has been compromised, the others probably are as well.

b. *Denial of service.* The most prevalent attack used against DoD systems is Denial of Service, where the attackers attempt to overwhelm a system to the point that it can no longer process legitimate traffic. There are basically three forms of this attack which must be safeguarded.
- Consumption of scarce, limited, or non-renewable resources;
- Destruction or alteration of configuration information; and
- Physical destruction.

APPENDIX A – ACRONYMS

AIS Automated Information System
AL Address List
C&A Certification & Authorization
CA Certificate Authority
CAW Certificate Authorization Workstation
CISSM Component Information Systems Security Manager
CKL Compromised Key List
COPS Computerized Oracle Password Systems
COTS Commercial-off-the-shelf Software
CMI Certification Management Infrastructure
CRL Certificate Revocation List
DAA Designated Approval Authority
DIA Defense Intelligence Agency
DII Defense Information Infrastructure
DISA Defense Information Systems Agency
DISC4 Director of Information Systems for Command Control Communications and Computers
DMS Defense Message System
DN Distinguished Name
DNS Domain Name Service
DoD Department of Defense
DSS Digital Signature Standard
FTP File Transfer Protocol
GOSC Global Operations and Security Center
GWS Groupware Server
HAG High Assurance Guard
I&A Identification & Authentication
IAS Information Assurance Solutions
IASO Information Assurance Security Officer
IAVA Information Assurance Vulnerability Alert
IT Information Technology
JS Joint Staff
KEA Key Exchange Algorithm
KMI Key Material Identifier
LAN Local Area Network
LOI Letter of Instruction
MFI Multi-Function Interpreter
MLA Mail List Agent
MS Mail Exchange
MS Message Store
MSP Message Security Protocol
MTA Message Transfer Agent
MTS Message Transfer System
NSA National Security Agency
NSO Network Security Officer
ORA Organizational Registration Authority
ORIM Office of Information Resource Management
OS Operating System
PAA Policy Approval Authority
PCA Policy Creation Authority
PGWS Primary Groupware Server
PIN Personal Identification Number
PUA Profiling User Agent
RA Registration Authority
RPC Remote Procedure Calls
SA Systems Administrator
SFUG Security Features User's Guide
SM Security Manager
SMTP Simple Mail Transfer Protocol
SNS Secure Network Server
SORA Sub-Organizational Registration Authority
SPECAT Special Category
SRA Subordinate Registration Authority
ST&E Security Test & Evaluation
TDY Temporary Duty
UA User Agent
VAAP Vulnerability Analysis Assessment Program

APPENDIX B -- GLOSSARY

Access. A specific type of interaction between a subject and an object that results in the flow of information from one to the other.

Access Control. The process of limiting access to the resources of a system only to authorized programs, processes, or other systems (in a network). Synonymous with controlled access and limited access.

Access Level. The hierarchical portion of the security level used to identify the sensitivity of data and the clearance or authorization of users. Note: The access level, in conjunction with the nonhierarchical categories, forms the sensitivity label of an object. See category, security level, and sensitivity label.

Accountability. The property that enables activities on an AIS to be traced to individuals who then may be held responsible for their actions. In COMSEC, the principle that an individual is responsible for the safety and security of COMSEC equipment, keying material, and information entrusted to personal care, and is answerable to proper authority for the loss or misuse of that equipment or information.

Accreditation. A formal declaration by the DAA responsible for a system that the AIS is approved to operate in a particular security mode using a prescribed set of safeguards based on the certification process and other management considerations. The accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security.

Address List. A single message address that acts as a collective address. When the message originator transmits the message to a mail list as the recipient name, the MLA is the address.

Administrative Directory User Agent. A software function that provides the means for an authorized person to enter, modify, or delete data in the DIB.

Audit. The independent review and examination of a system's records and activities to test for adequacy of the system's controls, to ensure compliance with established policy and operational procedures, or to recommend any needed changes in controls, policy, or procedures.

Audit Trail. A chronological record of system activities sufficient to enable the reconstruction, review, and examination of a sequence of environments and activities surrounding or leading to an operation, procedure, or event in a transaction from inception to final results.

Authenticate. To verify the identify of a user, device, or other entity in a computer system, or to verify the integrity of data that were stored, transmitted, or otherwise exposed to possible unauthorized modification.

Authentication. A security measure designed to protect a communication system against acceptance of fraudulent transmissions or simulation by establishing the validity of a transmission, message, or originator, or a means of verifying an individual's eligibility to receive specific categories of information.

Automated Information System. Any assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, or control data or information in an electronic form. AISs include stand-alone computers, small computers, word processors, multi-user computers, terminals, and networks. An Automated Information System is the same as an Information Technology System.

Information Systems Security. Measures and controls that protect an AIS from denial of service and unauthorized disclosure, modification, or destruction of the AIS and/or data.

Backbone Message Transfer Agent. The message switching and routing component of the DMS backbone.

Category. A restrictive label applied to classified or unclassified data to increase the protection of the data by further restricting access to it. Individuals are granted access to categories of information only after being granted formal access authorization.

Certificate Revocation List. A list of X.509 certificate serial numbers whose identity to key binding is no longer valid.

Certification. The comprehensive evaluation of the technical and nontechnical security features of an AIS, and other safeguards made in support of the accreditation process, that establishes the extent to which a design and implementation meet applicable security requirements.

Certification Authority. A person responsible for issuing user certificates, for placing certificates in the Directory, for generating and issuing PINs and for programming FORTEZZA cards.

Certification Authority Workstation. The workstation used by the CA.

Classified Defense Information. Official information regarding the national security that has been designated "TOP SECRET", "SECRET", or "CONFIDENTIAL" according to Executive Order 12356.

Commercial, Off-the-Shelf. An item that was produced and is available for purchase by the general public.

Component. A software process or a combination of a software process and the associated hardware platform that performs a service in preparing, transmitting, or translating messages.

Compromised Key List. A list of KMIDs assumed to have been compromised.

Communications Security. Measures taken to deny unauthorized persons any information derived from U.S. Government communications and systems to ensure the authenticity of communicated information.

Compromising Emanations. Unintentional intelligence-bearing signals that, if intercepted and analyzed, disclose the information that was transmitted received, handled, or otherwise processed by any information processing equipment.

Computer. A machine capable of accepting data, performing calculations on or otherwise producing, manipulating, and storing data.

Confidentiality. The concept of protecting data from unauthorized disclosure.

Configuration Control Board. A body that sets system standards and acts to control the configuration of a system by approving or disapproving submitted requests for a change to the system. The CCB also is responsible for checking additional impacts that might occur as a result of one change in an area of a system.

Configuration Management. A discipline applying technical and administrative direction and surveillance to identify and document the functional and physical characteristics of a configured item, to control changes to those characteristics, and to record and report changes to processing and implementation status.

Controlled Access Protection. Access control through log-in procedures, audit of security-relevant events, and resource isolation,

Data Integrity. Protection against the unauthorized modification of data, whether by change, deletion or insertion.

Database. A structured or organized collection of information.

Database Management System. A computer application that accesses or manipulates a computerized database.

Defense Information Infrastructure. A seamless web of communications networks, computers, software, databases, applications, and other capabilities that meets the information processing and transport needs of DoD users in peace and crises.

Defense Information System Network. A sub-element of the DII, this network is DoD's consolidated worldwide enterprise-level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations.

Denial of Service. Action or actions that prevent any part of an AIS from functioning to its intended purpose.

Designated Approving Authority. An organizations Chief Information Officer, who has the authority and responsibility to decide to accept or reject the security safeguards prescribed for an AIS, and who is responsible for issuing an accreditation statement or certificate that records the decision to accept those safeguards for the organization.

Digital Signature. A nonforgeable transformation of data that allows proof of source, nonrepudiation, and verification of data integrity.

Directory. A collection of open systems cooperating to provide Directory service. As used in DMS, the Directory is based on the ITU-T X.500 recommendations.

Directory Information Base. Information that exists in the Directory.

Directory Information Tree. The organizational model that employs a hierarchical tree structure.

Directory User Agent. The Directory User Agent communicates with the DSA in order to obtain or manipulate Directory information for its associated component or user.

Directory System Agent. The DSA serves to retain and make available a part of the DIB. It is accessible by any component that requires Directory information by means of a Directory User Agent.

Distinguished Name. A name that is unique in the entire global Directory.

Firewall. A type of access control gateway that is placed between a private or restricted access network and any other network to selectively filter incoming and/or outgoing traffic. Firewalls enhance network and application security.

FORTEZZA. The name given to the PCMCIA card employed in the encryption and authentication of DMS messages.

Gateway. A device for converting a message originated in the format and protocol of one network to the format and protocol of another network without changing the content or intent of the message text. A Gateway can be implemented in hardware or software.

Global Control Center. The DISA global facility that provides technical control and monitors the system and network integrity of the DII.

Global Service Manager. The operations manager for DMS at the global level who provides operational control and management direction over DMS.

Information Systems Security. A composite of means to protect telecommunications systems and AISs and the information processed.

Defense Message System. All hardware, software, procedures, standards, security services, facilities, and personnel used to exchange

messages electronically between organizations and individuals in DoD. The DMS relies on the DISN for data transfer.

Information Systems Security Officer. The individual responsible for enforcing security policies and doctrines related to an AIS.

Infrastructure. The underlying framework or supporting structure of any system. In this document, it includes the processors, operating systems, applications software and standards for DMS.

Integrity. The degree of protection for data from intentional or unintentional alteration or misuse.

Inter-operability. The ability of two or more systems or components to exchange and use information or services to operate effectively together.

Life-Cycle Management. Management of a system from design through program termination. It includes initial procurement, procurement and management of spare and repair parts, oversight of the maintenance process, configuration control, planning for improvements, collection of failure data, analysis, and support process modification, and proper disposal action at the end of the life cycle.

Local Area Network. A data network, usually locally on its user's premises in a geographical area.

Local Control Center. The facility at a site that provides technical control and monitors the system at the local level.

Local Service Manager. The operations manager at the local level who provides operational control and management direction over DMS at the site.

Mail List Agent. A DMS component that accepts messages addressed to MLs and re-addresses them to the individual recipients who are members of the address list.

Management Workstation. The MWS is the primary tool for network management at all management levels. It can receive, correlate, and distribute management information sent to it by managed network components.

Multilevel Information Systems Security Initiative. A set of solutions that provide security inter-operability and services among a wide variety of missions of the DII.

Multi-Level Security Mode. A mode of operation wherein not all users of the AIS possess the required personnel security clearance for all data being processed by the AIS.

Network. Communications medium and all components attached to that medium whose function is the transfer of information. Components may include AISs, packet switches, communications controllers, key distribution centers, and technical control devices.

Nonrepudiation. A process that protects against an attempt by a message originator to falsely deny responsibility for the sending of a message or for its contents.

Organizational Registration Authority. An appointed users and DMS certification and registration hierarchy. The primary function of the ORA is user identification and administrative validation of forms. The ORA gathers local information, accesses the Directory to verify the uniqueness of the user's Distinguished Name, and sends the request to the SRA and CA for action.

Private Key. A cryptographic key used in a dual key system, uniquely associated with an entity, and not made public. It is used to generate a digital signature. This key is linked mathematically with a corresponding public key.

Public Key. A cryptographic key used in a dual key system, uniquely associated with an entity, and made public. It is used to verify a digital signature. This key is linked mathematically with a corresponding private key.

Regional Operations and Security Center. The facility in a region that provides technical control and monitors the system at the regional level.

Regional Service Manager. The operations manager for the region who provides operational control and management direction over the DMS at a regional level.

Risk. The probability that a particular threat will exploit a particular vulnerability of an AIS.

Risk Assessment. The process of identifying security risk based on an analysis of threats to and vulnerabilities of systems, determining the magnitude of those risks, and incorporating measures needed to safeguard against them.

Simple Network Management Protocol. A standard protocol used to monitor Internet Protocol gateways and the networks to which they attach.

Simple Mail Transfer Protocol. A protocol for transferring electronic mail messages from one host to another. SMTP specifies how two mail systems interact and the format of control messages they exchange to transfer mail.

Sub-Registration Authority. The SRA works with the CA in developing a unique Distinguished Name for the user or entity on a FORTEZZA card, and creates an entry in the Directory for each personality associated with the user or

TEMPEST. The investigation, study, and control of compromising emanations from electrical and electronic equipment. TEMPEST is often used as a synonym for compromising emanations as in "TEMPEST test" or "TEMPEST inspection".

Threat. Any capability, circumstance, or event with the potential to cause harm to a automated information system in the form of destruction, unauthorized disclosure, modification of data, or denial of service.

Users. People or processes accessing DMS either by direct connections (i.e., via terminals) or indirect connections (i.e., preparing input or receiving output from the system without a review for classification or content by a responsible

individual).

User Agent. As defined in X.400, a software component of the MHS through which a single direct user engages in message handling. The UA assists users in preparing, storing, and displaying data.

X.400. The international recommendations developed by ITU-T for a message handling system in a multi-vendor environment.

X.500. The international recommendations developed by ITU-T for directory services for electronic mail.

Zeroize. The reformatting of a FORTEZZA card to eliminate outdated or compromised information.

APPENDIX C – REFERENCES

ACP 123 US Supplement, 30 March 2000

AR 25-AI

AR 25-AI-1

Army Letter of Instruction AR-25ops

Army Regulation 25-AI Information Assurance

Computer Security Act of 1987

D6/JIEO Information Systems Security Handbook, D614 Information Management, August 1999

DA PAM 25-IA

DISA Letter DMS Component Approval Process, 24 March 1993

DISAI 240-110-8.

DMS Security Features User's Guide, Defense Information Systems Agency, 7 October 1999

DMS Site Security Operation Procedures, 29 May 1998

DoD 5200.2-R, Personnel Security Program

DoD Information Technology Security Certification and Authorization Process (DITSCAP)

Information Systems Security for Managers, Defense Information Systems Agency

NAG 69B Information System Security Policy and Certification Practice Statement for Certification Authorities, National Security Agency

SDD Firewall Report 1, DMS Component Interactions, Services, and Protocols

SDD Firewall Report 2, Recommended DMS Architectural Solutions for Firewalls

SDD Firewall Report 3, DMS Commercial Firewall Study

Operations Working Group Security Briefing

AFIWC Security Assessment

Defense Message System (DMS)
Security Features User's Guide
(Final Draft)

Document Version 1.1

29 May 1998

Prepared for:
Defense Information Systems Agency
Defense Message System Program Management Office
5111 Leesburg Pike, Suite 900
Falls Church, VA 22041

by

J. G. Van Dyke & Associates, Inc.
5510 Cherokee Avenue, Suite 300
Alexandria, VA 22312

Defense Message System
Security Features User's Guide
(Final Draft)

Chapter 2 introduction

Purpose

The purpose of this Defense Message System (DMS) Security Features User's Guide (SFUG) is twofold.
First, it is a generic security guide for DMS end-users. As such, it is designed to provide the end-user with the understanding of his/her security responsibilities for the DMS. In addition, it provides the end-user with specific information regarding the DMS security features that will help him/her better perform his/her security responsibilities.
Second, it is a shell for use by the Site's DMS Security Official in creating a site-specific DMS SFUG. If the Site's DMS Security Official is satisfied that this generic DMS SFUG meets the site's requirements for an SFUG, it may be used as is. On the other hand, it may be tailored to meet the site's specific needs or replaced with another SFUG.

Scope

This DMS SFUG is written for end-users of the DMS User Agents (UAs). It is not intended to be a SFUG for DMS components such as the Certification Authority Workstation (CAW), DMS Guard, Directory Service Agent (DSA), Mail Transfer Agent (MTA), Mail List Agent (MLA) or Profile User Agent (PUA), etc. The user manual for each DMS component, other than the UA, is considered that component's SFUG.
It is presumed that each site has in place an appropriate document describing the site's information system security policy and security operational procedures. Therefore, this DMS SFUG does not include specific end-user security responsibilities that are standard to all sensitive and classified information systems (e.g., how to mark and handle sensitive and classified computer media, how to correct inadvertent placement of classified information on unclassified media, how to conduct virus checking). It does, however, provide guidance for placing per-body-part security labels on message body parts based on Allied Communications Publications (ACP) 123 [3] and ACP 123 US SUPP-1 [2].
The SFUG is not a technical manual. It should be used in conjunction with the end-user's DMS manual(s) to ensure secure user configuration and operation of DMS user agents.

Document Organization

Section 1 describes the purpose and scope of this DMS SFUG. It also gives the reader an overview of the document's organization.
Section 2 gives the reader a high level description of the DMS, describes the DMS philosophy of protection, lists useful definitions, and briefly describes the role of the DMS Information System Security Manager or Officer (ISSM/ISSO) and his/her relationship with the DMS end-user.
Section 3 describes the DMS end-user's security responsibilities.

Chapter 3 system security overview

This section is designed to give the end-user of DMS,

- A high level overview of the DMS,
- A general description of the DMS philosophy of protection emphasizing personal security responsibilities, and
- The use of FORTEZZA services to aid end-users in meeting their security responsibilities.

Also included is a list of definitions designed to assist end-users in understanding the terms used throughout this SFUG.

DMS Overview

For more than thirty years, AUTODIN has provided the Department of Defense (DoD) with unprecedented messaging support. Although the system has undergone numerous enhancements, its basic framework is late 1950's proprietary architecture. Consequently, it cannot be easily upgraded to support today's information requirements.
To meet today's information needs, DoD developed the Defense Message System (DMS) based on the commercially available e-mail system model. It is designed to meet DoD messaging requirements for functionality, speed, security, reliability, flexibility, and interoperability.
DMS incorporates two types of messages: organizational and individual.

An organizational message is a military message sent in the name of the organization. It establishes a formal commitment on behalf of that organization and has been formally released in accordance with the originating organization's policies. The organizational message requires approval by a designated authority from the originating organization for transmission. The receiving organization must determine internal distribution.

An individual message is a message sent from one individual to one or more other individuals. Individual messages can be compared with correspondence traditionally sent between individuals using commercial e-mail. The individual message identifies the originator (writer) and recipient(s) (reader) by name. Individual messages are appropriate for official business but do not establish a formal commitment on behalf of an organization.

DMS standardizes the distinction between organizational and individual messages and allows users to choose whether the message will be organizational or individual. Because organizational messages officially commit commands to actions or policies, the requirements for traceability, confidentiality, and integrity are generally more stringent than those of individual messages.

The DMS consists of a set of commercial-off-the-shelf (COTS) applications that provide a full range of messaging and security services. DMS is designed to allow end-users to both send and receive organizational and individual messages from their desktop or remote dial-in computers.

DMS Philosophy of Protection

As the DoD message system, the DMS must be secure. The main DMS objective is to operate all DMS-related applications and processes at an acceptable level of risk. In order to meet this objective, DMS employs four primary security services. They are:

- *Confidentiality* - the security service that ensures data is not made available or disclosed to unauthorized individuals, entities, or processes. For DMS, confidentiality extends to all data directly associated with DMS applications and processes including DMS messages, directory information, and management information.
- *Integrity* - the security service that ensures data, services, and other controlled resources have not been altered or destroyed in an unauthorized manner. For DMS, integrity extends to distribution determination and delivery services in addition to DMS messages, directory information, and management information.
- *Availability* - the security service that ensures resources, services, and data are accessible and usable on demand or in a timely manner by an authorized user or process. For DMS, availability extends to connectivity, inter-operability, survivability and guaranteed delivery, and timely delivery services.
- *Accountability* - the security service that enables activities to be traced to users and processes that may then be held responsible for those actions. For DMS, accountability includes the security services of identification and authentication, and extends to all data directly associated with DMS applications and processes including DMS messages, directory information, and management information.

As the primary writer-to-reader security service, DMS uses National Security Agency's (NSA's) Multilevel Information Systems Security Initiative's (MISSI's) FORTEZZA Technology. FORTEZZA technology provides DMS with:

- Confidentiality and integrity through encryption;
- Non-repudiation through digital signatures;
- Authentication through a combination of the FORTEZZA card itself and card's assigned Personal Identification Number (PIN) as well as digital signatures; and
- Access control by allowing the assigned FORTEZZA cardholder only to gain access to signed and encrypted messages addressed to that FORTEZZA cardholder.

The above four security services and FORTEZZA build on the foundation of each organization's established security policies, procedures, and practices to provide a secure DMS. Like any other security program, however, the most important ingredient for a secure DMS is the end-user.

DMS end-users have certain responsibilities to ensure that the DMS operates in a secure manner. The end-user's responsibilities include:

- Complying with the site's DMS security policies and procedures;
- Maintaining the security posture of the DMS operating environment;
- Reporting all Automated Information System- (AIS) and DMS-related security incidents and vulnerabilities to the site ISSM/ISSO;
- Complying with the site's access authorization procedures;
- Completing AIS and DMS security training;
- Avoiding fraud, waste, and abuse of the site's AIS and DMS resources; and
- Providing input to AIS security surveys and accreditation documentation as required by the site's security personnel.

Section 3 of this SFUG specifies DMS-related end-user security responsibilities and guidance.

Definitions

The following definitions will assist the end-user in understanding terms used elsewhere in this document.

Access Control: Procedures or mechanisms that restrict use of a computer system to authorized persons and processes only. For the DMS this includes restrictive mechanisms that permit only authorized users or processes to send or receive DMS messages and that limit the transmission of classified messages to those users and processes authorized to receive them.

Accountability: The DMS security service that enables activities to be traced to users and processes that may then be held responsible for those actions.

Audit: The act of gathering usage information on a computer system with the intent of detecting and deterring penetration of the system and revealing usage that identifies misuse.

Authentication: The process by which a user or process validates a claimed identity. (See identification.)

Availability: The DMS security service that ensures resources, services and data are accessible and usable on demand or in a timely manner by an authorized user or process.

Certificate: A computer based record that binds a subscriber's identify in the form of a Distinguished Name (DN) (and some authorizations) with their public key in a trustable association. The certificate identifies the Certification Authority (CA) issuing it, identifies its subscriber, contains the subscriber's public key and is digitally signed by the issuing Certification Authority.

Certificate Revocation List (CRL): A list containing certificates still within their validity interval, but that no longer represent a valid binding between a public key and a Distinguished Name or privilege. CRLs are created by all certificate-issuing authorities and are posted to the Directory.

Certification Authority (CA): A CA registers end-users (including machines) and issues their certificates. A CA is the MISSI administrative authority for an autonomous organization, or major unit of an organization, within a policy domain. The term CA refers to the authoritarian office or role as well as the person who fills that office.

Compromised Key List (CKL): A list generated by a Policy Creation Authority (PCA) that contains the Key Material Identifiers (KMIDs) of keys believed by the PCA to be compromised (i.e., no longer trustworthy).

Confidentiality: The DMS security service that ensures data is not made available or disclosed to unauthorized individuals, entities, or processes.

Digital Signature: A non-forgeable transformation of data that allows proof of source, non-repudiation, and verification of data integrity. For DMS, the digital signature is generated using the private key (see private key) and verified using the public key (see public key). The FORTEZZA card contains the user's private key.

Directory: An on-line repository of certificates, CRLs and CKLs.

Distinguished Name (DN): A unique identifier for all users in DMS. The DMS DNs include Country Name (C), an Organizational Name (O), and Organizational Unit (OU), and a Common Name (CN).

DMS User: As used in this document, A DMS user is the end-user that originates or receives a DMS message.

DMS Information System Security Manager or Officer (ISSM/ISSO): An organizational manager or officer who is responsible for the organization's adherence to DMS related security policies and regulations. Duties generally include preparing Organizational System Security Plans, examining and analyzing security audit trails, managing system user accounts, and reporting on and recommending fixes for any security discrepancies discovered.

FORTEZZA Card: A personal computer card that uses National Institute of Standards and Technology (NIST) and National Security Agency (NSA) approved algorithms and procedures to provide network related security services. The card when used in conjunction with the proper applications and network infrastructure, provides data integrity, access control, authentication, non-repudiation and confidentiality of user information. The FORTEZZA card is an integral part of the Multilevel Information System Security Initiative (MISSI). The Personal Computer Memory Card International Association (PCMCIA) card is employed in the encryption and authentication of DMS messages.

Encryption: A process that disguises a message in such a way that its contents or substance is hidden or unintelligible. DMS uses the FORTEZZA card for encryption.

Identification: The means by which a user or process provides a claimed identity to a computer system. A user ID is an example of identification.

Integrity: The DMS security service that ensures data, services, and other controlled resources have not been altered or destroyed in an unauthorized manner.

Key Material Identifier (KMID): A globally unique field contained in a DMS certificate that identifies a specific set of private key material. The Policy Creation Authority (PCA) uses the KMID when generating the CKLs.

Message Release Authority: A designated authority within an organization that has approval authority to release organizational messages.

MISSI: The National Security Agency's Multilevel Information System Security Initiative.

Non-Repudiation: In a message system, any process that protects against an attempt to falsely deny or repudiate responsibility for the origination, content or receipt of a message. DMS uses a digital signature for non-repudiation.

Originator: The individual or organization that originates a DMS message.

Organization Registration Authority (ORA): An ORA is a local MISSI administrative authority who assists a CA with registering end-users by gathering end-user registration information and forwarding it to the CA. An ORA does not sign certificates or CRLs.

Organization Security Manager or Officer: The organizational manager or officer who is assigned the overall security responsibility for that organization.

Password: A unique set of alphanumeric and special characters assigned to or created by a user for use in authenticating the user when logging in to a computer system or application.

Personal Identification Number (PIN): A random multiple digit number assigned to the FORTEZZA card. The PIN is required to activate the FORTEZZA card.

Public Key: One of two related keys (public and private) used in a cryptographic key pair. Anything encrypted using one of the two keys can only be decrypted with the other key of the pair. The public key is made public. For the DMS, the originator's public key is used to verify the originator's digital signature, which is generated with the originator's private key. (See private key.)

Private Key: One of two related keys (public and private) used in a cryptographic key pair. Anything encrypted using one of the two keys can only be decrypted with the other key of the pair. The private key is kept confidential. For the DMS, the originator's private key is used to digitally sign a message or receipt. The recipient uses the originator's public key to verify the digital signature. (See public key.)

Recipient: The individual or organization that receives a DMS Message.

Removable Media: Computer media that is easily removed from a computer, such as floppy diskettes, tapes, removable hard disk drives, CD ROMs, etc.

Security Incident: An actual or suspected event or incident, intentional or accidental, that places the security of a computer system, or sensitive or classified information at risk. A security incident could result in a breach of confidentiality, data or system integrity, or availability.

Signed Receipt: A digitally signed receipt that signifies that a DMS message was received and the receipt of which cannot be denied (non-reputiation).

Trojan Horse: A program that performs a desired task, but that also includes unexpected (and undesirable) functions. Consider as an example, an editing program for a multi-user system. This program could be modified to randomly delete one of the user's files each time they perform a useful function (editing), but the deletions are unexpected and definitely undesired.

Virus: A computer program that embeds itself in other code and can replicate itself. Once active, it takes undesired and unexpected actions that can result in either destructive or non-destructive outcomes in the host computer.

Worm: A self-replicating program that is self-containd and does not require a host program. The program creates a copy of itself and causes it to execute thus replicating itself again and again; no user interaction is required. Worms commonly use network services to propagate to other host systems.

The DMS Information System Security Manager or Officer (ISSM/ISSO)

DMS Security Policy requires each DMS site to have an Information Systems Security Manager or Officer (ISSM/ISSO). The ISSM/ISSO is the person responsible for enforcing DMS site security policies and procedures. The ISSM/ISSO, or designee, is the person the end-user should interact with for most DMS security related issues. He/she is the person the end-user should contact if he/she has any DMS related security questions or concerns. Normally, the ISSM/ISSO, or designee, is the person the end-user reports DMS security incidents to.

The ISSM/ISSO responsibilities may vary slightly at each location, but the below listed responsibilities are typical.

- Being the focal point for all assigned system, directorate, or department DMS security matters;
- Implementing the DMS AIS security program as it applies to site-specific AIS, including preparing and submitting accreditation support documentation;
- Maintaining an inventory of all DMS hardware, implemented system software releases, and major functional application systems;
- Monitoring system activity, including identifying the levels and types of data handled by the AIS, verifying password assignments, and reviewing audit trails, outputs, etc., to ensure compliance with DMS security policies and procedures;
- Conducting and documenting the site DMS risk assessment;
- Coordinating all system security matters with DMS security management structure , and system users;
- Completing an AIS security survey for DMS and participating in the preparation of the customized Site Security Operational Procedures (SSOP);
- Supervising, testing, and monitoring changes affecting the AIS activity and network security posture;
- Implementing appropriate safeguards required by directive;
- Monitoring system activity for security violations and reporting all security infractions;
- Supporting user training in correct AIS security procedures; and
- Assisting in the implementing, developing, and testing the site DMS contingency plan.

Chapter 4 the dms user security responsibilities

The DMS incorporates many security features (see section 2 of this document) to ensure writer-to-reader security. However, without each DMS end-user meeting his/her security responsibilities, DMS security is incomplete. Section 2.2 of this document gives an overview of the DMS philosophy of protection and highlights security responsibilities for an end-user.

This section gives specific DMS security guidance and identifies specific security responsibilities for a DMS end-user. In addition, the end-user may have other DMS and AIS security responsibilities that are specific to his/her organization. The end-user should consult the site ISSM/ISSO for specifics.

User Initialization of DMS User Agent

The user may configure certain DMS User Agent (UA) security features. They include, whether or not entering the FORTEZZA card PIN is required for each message, the length of time before the FORTEZZA card times out when idle, certain audit features, configuring UAs for directory searches and user selection of the DMS UA password. General guidance for configuring UAs for directory searches and user selection of the DMS UA password is given below. The user should reference local security policy and procedures for guidelines for other DMS UA configuration.

It is important for the user to follow local security policy when performing any configuration of the DMS UA. It is also important that the user not alter the initial DMS UA configuration unless specifically authorized to do so by local security policy.

Configuring UAs for Directory Searches

The Global DMS Directory contains current addressing and security information required to send a DMS message to individuals and organizations. The most flexible way to access the directory is by using the Directory Information Tree (DIT) browser icon from the Windows desktop. The DIT browser can be configured by the user to display their choice of their highest level of the tree that could result in quicker directory searches.

User Password Selection Guidance

The most common technique used to gain unauthorized system access involves password guessing sometimes called password cracking. Password cracking is a technique used to secretly gain system access by using another user's account. Users often select weak passwords that could easily be guessed by knowing a little something about the user (e.g., wife or children's name) or passwords susceptible to dictionary attacks (i.e., brute-force guessing of passwords using a dictionary as the source of guesses). It is the user's responsibility to choose a password that follow the guidelines listed in the site's local security policy. Below is a list of suggested guidelines to be used when selecting and protecting your password:

- Pick passwords that aren't words or names, but choose a password that is easy for you to remember,
- Pick a mix of alphabetic and numeric characters, and use at least one special character,
- Passwords should be at least 6 characters in length,
- Don't keep passwords that may have come with your system,
- Don't ever let anyone use your password,
- Don't write your password down unless it is safeguarded commensurate with its sensitivity or classification level,
- Don't type a password while anyone is watching,
- Don't record your password on line or send it anywhere via electronic mail, and
- Change your password in accordance with local security policy.

FORTEZZA Security Services

FORTEZZA security services allow the user to encrypt or digitally sign, or both, individual and organizational messages. The end-user that is authorized to use FORTEZZA security services is issued a FORTEZZA card containing the necessary tools that allow him or her to encrypt and digitally sign DMS messages. The user may receive a FORTEZZA card for use with unclassified and sensitive but unclassified messages or SECRET messages or both. In some cases the user may have separate FORTEZZA cards: one for unclassified and sensitive but unclassified messages only, the other for SECRET messages only.

In addition, a FORTEZZA card may be an individual card or an organizational card. An individual card is assigned to a specific person and should not be shared with another person. An organizational card represents an organization opposed to a specific person. Multiple authorized people, as determined by local security policy, may share an organizational card.

The FORTEZZA card contains encryption algorithms that are regulated by the National Security Agency (NSA). The following paragraphs describe the user's security responsibilities associated with FORTEZZA security services available to the DMS. Specific security policy for end-users should be available from the Organization's ISSO or Certification Authority (CA).

FORTEZZA Card Access Controls

Access to FORTEZZA security services requires a user's Personal Identification Number (PIN), a FORTEZZA card, and a hardware or software application enabled to invoke the card's services. The FORTEZZA sensitive but unclassified (SBU) card is authorized for use with unclassified and SBU information only. The FORTEZZA SECRET card may be authorized for use with SECRET information only or may be authorized for use with unclassified and sensitive but unclassified information as well as SECRET information.

The user enters a PIN when requested by the DMS User Agent (UA) to enable or "unlock" the FORTEZZA card. The FORTEZZA card when removed from the computer is considered inactive or "locked".

Since it is the PIN that enables the FORTEZZA, when the FORTEZZA card is locked it is unclassified. However, both the PIN and the FORTEZZA card, even when locked, must be afforded proper protection against unauthorized access.

Safeguarding Personal Identification Numbers (PINS)

Personal Identification Numbers should be memorized. PINs must not be written on the FORTEZZA card or recorded in any manner in the vicinity of the host system for any reason. Doing so could result in an unauthorized person enabling or unlocking the FORTEZZA card.

The PIN letter (the letter the user receives notifying him or her of his or her PIN) or any other written record of the PIN should be securely stored separate from the FORTEZZA card. Secure storage of a written record of the PIN should be commensurate with the FORTEZZA card's classification level. For an unclassified and sensitive but unclassified card, at minimum, safeguard the PIN to adequately protect against loss or unauthorized access.

Safeguarding the FORTEZZA Card

The FORTEZZA SBU card is not classified but must be afforded adequate safeguarding. When a FORTEZZA SECRET card is locked it is unclassified, but must be physically protected.

Safeguard locked FORTEZZA cards in a manner similar to a credit card or high value item to limit the possibility of loss, unauthorized use, substitution, tampering, and breakage. Equivalent protection should be applied during periods of non-use such as vacations, leave periods, etc. to help prevent possible unauthorized use.

Local security policy determines if a person may carry a FORTEZZA card on his or her person away from the work area. Local security policy may require more stringent safeguarding methods than described above.

Applying for a SBU FORTEZZA Card

Application for a FORTEZZA card is determined by local security policy. The user should be prepared to provide the CA or the CA's representative with proper photo identification (e.g., government identification or driver's license) to establish the user's identity.

After the FORTEZZA card and PIN letter are received, each FORTEZZA card user must sign and date a FORTEZZA User Advisory Statement and Receipt. By signing the FORTEZZA User Advisory Statement and Receipt the user acknowledges receipt of the FORTEZZA card, PIN letter, and the user agrees to accept the certificates listed on the Certificate report provided with the FORTEZZA card.

Reportable Events

The following events involving FORTEZZA card usage should be reported to the CA/ORA and ISSO immediately for review and possible compromise recovery actions:

- Loss of Card – The temporary or permanent loss of any FORTEZZA card.
- PIN Compromise - Actual or suspected compromise of PIN.
- Card Misuse – Actual or suspected misuse of the FORTEZZA card and associated software (i.e. unauthorized modification to the FORTEZZA software installed on the host). This includes detection of unauthorized users or users with unapproved cards. Unapproved cards are those that have not been programmed and certificates issued and signed by a CA.
- Card Tampering – Actual or suspected tampering with the FORTEZZA card.
- Duplicate Cards – Unauthorized use of an authorized duplicate card.
- Personal Data Changes – Should any user data change, (e.g. changes in job status, employees leaving, certificate changes), advise the CA who will take action as appropriate.
- Card/PIN Not Received – If a programmed FORTEZZA card or PIN or both are not received from the CA/ORA.
- User Departure – FORTEZZA card users leaving an organization without advising the CA concerning the status of their card.
- Premature Disabling – If a user's card is disabled prior to the user making ten unsuccessful consecutive attempts to unlock their card (due to the possibility of an unauthorized user attempting to access a user FORTEZZA card).

Local security policy determines reporting procedures and format. However, reportable events should generally include the following information:

- User's name, distinguished name, card serial number (chip internal serial number) and organization;
- All certificates and CAs who programmed certificates on the card;
- Complete circumstances of incident, including physical security situations;
- Other personnel involved in the incident;

- What was compromised (the card, PIN, FORTEZZA software);
- User's assessment of degree of compromise.

Troubleshooting FORTEZZA Related Problems

Operational difficulties with the FORTEZZA card (e.g., faulty card, expiration of certificates) should be reported to the CA, the CA's representative, or other person designated by local security policy and procedures.

The FORTEZZA card will disable itself after ten ***consecutive*** failed attempts to enter the PIN. Users must contact their designated CA or CA's representative for a new PIN and card reactivation. Users must not attempt to repair or reprogram inoperable FORTEZZA cards. An inoperable card must be returned to the issuing CA who will determine if the card can be reused. If cards are not returned in person to the CA, the cards must be returned via controlled methods (see local security policy and procedures). If the card itself is defective, a new card, new certificate, and new PIN will be programmed for the user. To allow recovery of back traffic encrypted with the old certificate, the old certificate will be reprogrammed onto the new card. This will allow the user to recover and re-encrypt information from the old certificate to the new certificate. The CA will revoke the old certificates 30 days after re-issue.

There are a number of errors that may occur during the use of the FORTEZZA card. Table 3-1 below describes the error codes that the user may encounter and a description on how the user can correct the error. If following the recommended user action does not correct the problem or if any other error codes occur, contact the system administrator or CA for assistance.

Table 4-1 FORTEZZA Error Codes

Error Code	Description	User Action
-23	PCMCIA Socket Services is not loaded	Exit all applications and reboot PC. Ensure Fortezza card is in PCMCIA reader when rebooting.
-2	CI Library has not been initialized	Exit all applications and reboot PC. Ensure Fortezza card is in PCMCIA reader when rebooting.
9	The function may not be performed in this state	Exit the application. Make sure card is properly inserted in PCMCIA reader. Restart the application.
142	Error while calculating message hash	Exit the application. Make sure card is properly inserted in PCMCIA reader. Restart the application.
201	Missing _Token - Could not find token for recipient	Check to make sure that the role you have selected off the card matches that of the inbox you are logged in to. If your Fortezza card has been modified recently, the originator may be using a cached version of your old certificate from their address book.
590	A recipient's certificate is on the CRL	Remove that recipient's entry from your address book and retrieve this entry from the directory. If this does not resolve the error, this user may have had their access revoked.

Returning the FORTEZZA Card

Prior to departing an organization, or when possessing a FORTEZZA card is no longer required, the user must return the FORTEZZA card to the CA or the CA's authorized agent. Failure to return the FORTEZZA card will result in the CA reporting the card as compromised. This report may affect the ability for the user in obtaining another FORTEZZA in the future.

FORTEZZA Card Emergency Destruction Procedures

In the event that it is necessary to destroy a FORTEZZA card to prevent it from falling in the hands of an unauthorized person the user should reference the following guidelines.

FORTEZZA SBU cards do not require special emergency destruction because they are used with unclassified and sensitive but unclassified information only. Based on NSA policy, a locked FORTEZZA SBU card is adequate protection. Check local security policy for more stringent requirements.

FORTEZZA SECRET cards should be physically destroyed in the event of an emergency by breaking it in half, or by pounding with a hammer or other heavy object.

Physical Security

Each organization incorporates certain physical security controls, policies, and procedures to prevent unauthorized access to sensitive or classified areas and information. Organizations also use physical security to protect physical property and personnel.

The DMS end-user should take advantage of the physical security controls that are available at his/her facility to protect the DMS and related sensitive and classified information. Each location will have physical security policies and

procedures that are applicable to that facility and its unique environment. The end-user is responsible for complying with the following security guidelines as they apply to his/her facility and its site security policies and procedures. The end-user should:

- Protect sensitive and classified information against inadvertent access by unauthorized persons.
- Position their workstation screen so that unauthorized persons cannot view it when they are working on sensitive and classified information.
- Position the window blind or shade in his/her work space to preclude observation of their workstation, if there is a window in the work space and the workstation cannot be positioned to prevent someone outside from observing it.
- Verify that sensitive or classified information is not displayed or that his/her FORTEZZA card is not activated when leaving the workstation unattended. (Some circumstances or policies may require that an unattended workstation be secured.)
- Prohibit another person from using their workstation while his/her FORTEZZA card is activated unless that person is authorized to use that FORTEZZA card (i.e., an organizational card).
- Use approved containers or areas for storage of sensitive and classified information (e.g., printouts, removable media) when unattended.
- Properly mark and safeguard removable media that contains sensitive or classified information.
- Properly review all printouts for sensitive and classified content. He/she should properly mark and safeguard printouts that contain sensitive or classified information.
- Double-check the workstation and workspace when leaving it unattended or securing for the day to ensure that all sensitive and classified information is properly safeguarded.
- Follow site physical security policy regarding securing their workspace.

Personnel Security

Personnel security controls are designed to ensure that people are authorized to have access to sensitive or classified information before access is permitted. Each organization has specific personnel controls, policies and procedures based on established Department of Defense policy for access to sensitive and classified information.

The DMS end-user is personally responsible for ensuring that only authorized people gain access to sensitive and classified information under his/her control. The end-user is responsible for complying with the following guidelines as they apply with his/her facility and its site security policies and procedures. The DMS end-user should:

- Verify each person's, including visitors, access level, clearance level and/or need to know before giving access to sensitive or classified information.
- Take great care to ensure that maintenance personnel do not have access to sensitive and classified information unless specifically authorized.

Message Processing

The DMS user has certain specific responsibilities when processing outgoing and incoming messages. Guidance for those responsibilities is given below.

Verifying Distinguished Name (DN) and Aliases

When preparing and sending a message, ensure that the person or organization to which the message is addressed is in fact the intended recipient. Failure to do so may result in the message going to a destination that does not have a need-to-know for the information included in the message.

Maintaining Current CKLs and CRLs

The organization's CA is responsible for ensuring that Compromised Key Lists (CKLs) and Certificate Revocation Lists (CRLs) are kept up-to-date. The user is responsible for ensuring that the user's CKLs and CRLs are current. It is also important that the user use the CKLs and CRLs when both sending and receiving messages to ensure that the recipient or sender has valid certificates.

Signing and Encrypting Messages

It is the user's responsibility to sign, encrypt, or both, outgoing messages in accordance with local security policy. Both digital signature and date encryption are features of the FORTEZZA security services. See section 3.2 of this user's guide for further details.

Archiving User Copies of Messages

It is the user's responsibility to ensure that appropriate safeguards commensurate with the message's classification level are taken when archiving messages. If messages are archived by printing or storing on removable computer media, follow the guidelines located in section 3.7 of this user's guide.

See local security policy and procedures for specific guidance for archiving user copies of messages.

DMS Message Security Labels

The DMS end-user has two responsibilities for ensuring that outgoing messages receive proper security labels:

- Placing a security label on the message as a whole, and
- Placing security labels in each of the message body parts.

Body parts in a DMS message can be compared to the parts of a typical e-mail message that are thought of as the main textual body of the message and the message attachments. The main textual body of a DMS message and each attachment is considered a body part in DMS.

A DMS message can be made up of one or more body parts. But a DMS message is more than a collection of its body parts. A DMS message also contains header information and other parts, such as the digital signature. Therefore, a message in DMS includes all body parts, header information, and everything else that makes up the message as a whole.

Message Security Labels

When the originator creates a DMS message, the user agent (UA) graphical user interface (GUI) requests a classification level or security label for the message as a whole. This is the message security label. The message security label identifies the overall classification level for the message. The message security label will reflect the highest classification of any part of the message or the appropriate classification for the aggregate of the information contained in the entire message.

WARNING. If the message is not encrypted using the FORTEZZA services, the message security label placed in the GUI will ***not*** be transmitted with the message. Reference Service/Agency or local security policy for sending non-encrypted messages.

Specific guidelines for applying message security labels are defined by Service/Agency or local security policy. Message security labels are UNCLASSIFIED, CONFIDENTIAL, and SECRET. Security labels for higher classification levels will be available during future releases of the DMS.

The originator should always double-check the message security label after changes or additions are made to a message. This double-check is to ensure that the security label placed on a message accurately represents the highest classification level for the entire message.

Message Subject Line

The DMS user agent GUI contains space for the message originator to enter a message subject. Normally, the subject line should be unclassified.

Even if the message is encrypted using FORTEZZA services for purposes of confidentiality, ***the subject line may be passed in the clear*** when the message is transmitted across the network. Therefore, the GUI subject line should not contain classified information or information that the originator wishes to keep confidential.

Per-Body-Part Security Labels

When the originator creates a message it is his/her responsibility to ensure that all body parts (i.e., the main textual body of the message and all attachments) are properly marked with classification markings, including any special handling requirements[1]. The security label that is placed in each separate body part of a message is called a per-body-part security label. The per-body-part security labels are in addition to the DMS message security label.

The actual information in a military message (MM or P772 message) is located in the body of the message. This may be formatted as either a single body part or as multiple body parts. Unless an explicit military text format for the message body part has been specified (ADatP-3[2], USMTF[3]), a "free-formatted" text body part may be used.

This section provides general guidance for applying per-body-part security labels for the end-user based on ACP 123 [3] and ACP 123 US SUPP-1 [2]. Specific guidelines for applying per-body-part security labels, however, are defined by Service/Agency or local security policy.

Explicit Military Text Format Body Parts

Per-body-part security labeling for body parts that have an explicit military text format (ADatP-3, USMTF) should be applied as specified in the required format. For those explicit military text formats that do not provide space for a security label or classification level, the originator of the DMS message should include the appropriate security label.

The guidance in the next section, "Free-formatted" Text Body Parts, is also applicable when placing security labels in explicit military text format body parts that do not contain provisions for classification markings within that format.

"Free-formatted" Text Body Parts

"Free-formatted" text body parts may be used in a message with a single body part or in a multiple body part message. The security classification and appropriate special handling requirements for a "free-formatted" text body part, should be the first line of the text. This line should also contain appropriate international alliance prefix/designator (e.g., COSMIC, NATO, etc.)

Appropriate paragraph and portion markings should also be included for the remainder of the body part.

Single Body Part Messages

---

[1] Special handling requirements are also know as caveats, special handling instructions, or special handling designators.

[2] ADatP-3 refers to a class of military messages that have a predefined formatted text designed to convey information for commonly used and mission critical uses. Examples of ADatP-3 messages include Air Tasking Orders and logistics reports.

[3] United States Message Text Format

When a message contains a single body part, it should be either an explicit military text format body part or a "free-formatted" text body part. Per-body-part security labels for these kinds of body parts should be applied as explained above.

Multiple Body Parts

When a message contains multiple body parts, possibly with some of them in formats other than plain text (e.g., graphics, binary), the main textual body of the message (the first body part) should be, if at all possible, "free-formatted" text. If the first body part is an explicit military text format the information described in the next paragraph should precede the military text format.

This first line of the first body part should include a security label that reflects the highest classification level of any part of the message or the aggregate of the information contained in the entire message. The first body part security label should also contain all special handling requirements that are included in the other body parts. The security label (i.e., classification and special handling requirements) in the first body part represents the overall classification for the message content, similar to the way a document cover sheet or cover letter reflects the overall classification of a document. It is appropriate to include a security label such as, SECRET (UNCLASSIFIED when attachments removed).

This first body part should also provide an overview of the other body parts, action to be taken for each, and the classification level of each. A first body part with its descriptive information should also be present when all other body parts of the message are non-text body parts.

Each subsequent body part in a multiple body part message should prominently display its appropriate security classification as well as applicable special handling requirements, if any. When including a security label in the existing attachment is neither practical nor possible see the next section, Body Parts Without Per-Body-Part Security Labels.

Body Parts Without Per-Body-Part Security Labels

Some body parts, such as graphics or binary, do not contain applicable classification markings or appropriate special handling requirements. When including a security label to existing files is neither practical nor possible, appropriate precautions should be taken to identify its classification level and special handling requirements. For example:

- Including the proper classification level and special handling requirements in the main textual body of the message (see section 3.6.3.2 above).
- Indicating in the main textual body of the message that the body part in question does not contain an internal security label.

When body parts without internal per-body-part security labels are stored on computer storage media, appropriate precautions should be taken to identify the files proper classification level and special handling requirements. Examples include:

- Arranging files on the storage media by classification levels and special handling requirements.
- Segregating classified files and unclassified files into separate directories.
- Including a text file within each directory describing each file in that directory including classification level and special handling requirements.

Forwarding Messages

When forwarding a message, special attention should be given to both the message security label and the per-body part security labels and special handling requirements of the forwarding message as well as the forwarded message.

A forwarding message is a new message that contains the message to be forwarded plus any additional information or body parts or both. A forwarded message is the original message that the forwarding message will forward.

The security labels of the forwarding message should reflect the classification level and special handling requirements based on the information and body parts in the forwarding message as well as the forwarded message. The first body part and other per-body-part security labels and special handling requirements in the forwarded message should be changed based on changes to the forwarded message, if any.

Message Reply

When replying to a message, the reply may or may not include all of the body parts of the original message. Likewise, the reply may contain additional information or body parts, or both, that were not contained in the original message.

The security labels for a reply message should reflect the proper classification level and special handling requirements based on the information and body parts contained in the reply message.

Protection of Classified and Sensitive But Unclassified Information

It is the user's responsibility to handle and safeguard all information, both printed and that stored on computer media, commensurate with its classification level.

When printing messages, the user should review the message contents, including all attachments, to ensure that the message is properly marked with the appropriate classification markings. If not, the user should appropriately mark the message.

When storing sensitive and classified messages on removable computer media, the user should ensure that the computer media is properly marked, reflecting the highest classification level of any file on the medium or the aggregate of the information contained on the entire medium. Also include special handling requirements, if any.

Local security policy and procedures contain specific guidance for handling classified and sensitive information.

Security Incident Reporting

A computer security incident can result from a computer virus, other malicious code, system intruders, or inadvertent user activity, such as accidentally placing classified information on an unclassified system. Without immediate technical expert response, the DMS could result in severe damage or compromise of sensitive or classified information. Generally, the user should not take any corrective action, but immediately notify the appropriate person in his or her organization, such as the ISSO or Terminal Area Security Officer (TASO) for guidance and corrective action.

Refer to local security policy for the types of security incidents and the procedures in which to follow in the event one should occur.

System Audit Logs

The DMS user's involvement in the auditing is generally limited. However, the user needs to be aware that auditing is required by the DMS Security Policy and that auditing activities are being performed to protect the information resources that are used. In accordance with local security policy, certain audit features at the user agent should be turned on and audit logs should be maintained on line until collected by the ISSO.

Authorized Software

All software introduced on a user's system should be properly authorized in accordance with local security policy. Some software may conflict or have an undesirable impact on DMS software as well as other software on the user's system. Refer to local security policy regarding the entry of computer programs into the user's system as well as determining what is “Authorized Software.”

Malicious Logic

The computer systems are under attack from a multiple of sources. One of these is called malicious logic, such as computer viruses, worms, Trojan Horses, logic bombs and other “uninvited” software.

There are certain precautions that can be taken to prevent the spread of viruses and related threats. Follow your local security policy regarding the screening for computer viruses and other malicious logic. The following are signs to look for that may indicate that a system is infected:

- Programs attempting to write-protect media,
- Unexplained decrease in PC or workstation memory,
- Vanishing executable files,
- Unusual monitor displays and messages,
- Increases in the bad areas of disk and/or hard drives,
- Delays in program start-up,
- Unexpected rebooting,
- Outgoing mail that the user did not intend to send,
- Unexpected changes to volume labels,
- Unexplained slow-down in processing time, etc., and
- Unexpected links to another unauthorized program.