

20 MAY 2003



Communications and Information

**MANAGING AIR FORCE MESSAGING
CENTERS**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

OPR: HQ AFCA/GCOM (Maj Robert Schutt)

Certified by: HQ USAF/ILCS
(Lt Col Dean Clemons)

Supersedes AFI 33-113, 1 March 1998.

Pages: 26
Distribution: F

This instruction implements Air Force Policy Directive (AFPD) 33-1, *Command, Control, Communications, and Computer (C4) Systems* and is divided into three sections. This instruction provides procedures and assigns responsibilities for managing Air Force messaging centers (MC). MCs encompass support for legacy Automatic Digital Network (AUTODIN) messaging through the telecommunications centers (TCC) and the Defense Message System (DMS) in the local network control center. It identifies DMS as the core-messaging system of record for the Air Force. It outlines the Air Force strategy to operate and manage messaging support for Air Force bases worldwide and defines MC management, control, operational environment, responsibilities, basic security procedures, and several other related activities to ensure effective and efficient support for communications and information capabilities. "The *Paperwork Reduction Act of 1995* as amended in 1996 and Air Force Instruction (AFI) 33-360, Volume 2, *Forms Management Program*, affect this publication." Refer technical questions about this instruction to Headquarters Air Force Communications Agency (HQ AFCA/GCOM), 203 West Losey Street, Room 2110, Scott AFB IL 62225-5222. Send recommended changes or comments to HQ AFCA/ITXD, 203 West Losey Street, Room 1100, Scott AFB IL 62225-5222, through appropriate channels, using AF Form 847, **Recommendation for Change of Publication**, with an information copy to HQ AFCA/GCOM. **Violations of the prohibitions of paragraph 4.8.2. by military members constitute a violation of Article 92, Uniform Code of Military Justice (UCMJ), and may result in punishment under the UCMJ. Violations by civilian personnel may result in administrative or other disciplinary action under applicable civilian personnel regulations or instructions. Violations by contractor personnel will be handled according to applicable contract law.** Maintain and dispose of records created as a result of prescribed processes in accordance with Air Force Manual (AFMAN) 37-139, *Records Disposition Schedule*. The reporting requirement in this publication is exempt from licensing in accordance with paragraph 2.11.10 of AFI 33-324, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections*. Refer to **Attachment 1** for a glossary of references and supporting information.

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed.

It places DMS in the forefront as the core-messaging system of record for the Air Force. It provides concise roles and responsibilities for managing messaging centers within the Air Force. It establishes the requirement for the creation of site Base Distribution Points (BDP) and organization Traffic Service Station (TSS) account. It identifies site trouble and outage status reporting requirements. References to “Data Processing Centers” (which officially no longer exist in the Air Force) have been removed. Messaging user responsibilities have been removed and will be established in the next pending version of AFI 33-119, *Air Force Messaging Management and Use*. It eliminates guidance on Fault Management, Configuration Management, and Performance Management. This guidance is located in AFI 33-115, Volume 1, *Network Management*.

Section A	Roles and Responsibilities	3
1.	Roles and Responsibilities	3
Section B	Defense Message System Operational Policy and Guidance	8
2.	Policy and Guidance.	8
Table 1.	Message Precedence/Grade of Service.	8
Section C	Messaging Centers (MC)	9
3.	Standard Practices	9
4.	Operations Management	10
5.	Message Distribution Terminal (MDT) Operations	14
6.	Storage Media Management	15
7.	Facility Management	15
8.	Automatic Digital Network Plain Language Address and Address Indicator Group Transition in Defense Message System	16
9.	Addresses	16
10.	Information Collections, Records, and Forms or Information Management Tool (IMT)	16
Attachment 1— GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION		18
Attachment 2—DEFENSE MESSAGE SYSTEM TROUBLE & OUTAGE REPORTING		25

Section A—Roles and Responsibilities

1. Roles and Responsibilities .

1.1. Headquarters, United States Air Force, Director of Communications Operations (HQ USAF/ILC). HQ USAF/ILC has overall responsibility for management, control, planning, and programming currently operational messaging systems. The HQ USAF/ILC will:

- 1.1.1. Execute and manage planning, programming, budgeting, and implementation activities.
- 1.1.2. Ensure Certificate of Networkiness (CoN) is completed prior to fielding and implementation.
- 1.1.3. Function as the Air Force control authority for Address Indicator Groups (AIG), Plain Language Addresses (PLA), Version-1 Mail Lists (ML), and Version-3 Address Lists (AL).
- 1.1.4. Serve as the functional designated approving authority (DAA) in accordance with AFI 33-202, *Computer Security*.
- 1.1.5. Represent the Air Force in the DMS Implementation Working Group.
- 1.1.6. Conduct Training Planning Team meetings with AFCA, major command (MAJCOM), field operating agency (FOA), direct reporting unit (DRU), Defense Message System-Air Force (DMS-AF) Program Management Office (PMO), and Air Education and Training Command (AETC) to identify new training requirements. Develop course training plans and course training standards.

1.2. HQ AFCA, DMS-AF Lead Command. HQ AFCA, as lead command for Air Force messaging, in compliance with AFI 10-901, *Lead Operating Command--Communications and Information Systems Management*, develops operations policy and guidance. HQ AFCA will:

- 1.2.1. Provide messaging functional management and process operational requirements for deployed, intelligence, and strategic communities.
- 1.2.2. Develop acquisition, fielding, and support plans and strategies.
- 1.2.3. Formulate operational policies and procedures.
- 1.2.4. Establish standards or other measurements to evaluate performance.
- 1.2.5. Coordinate training requirements with HQ USAF/ILCX and the MAJCOM/FOA/DRU training managers.
- 1.2.6. Provide manpower staffing requirements for inclusion in the applicable manpower standard.
- 1.2.7. Coordinate security issues, policies, and procedures with National Security Agency, Defense Information Systems Agency (DISA), intelligence community, program management activities, and MAJCOMs/FOAs/DRUs.
- 1.2.8. Provide message preparation and transmission guidance to the MAJCOMs/DRUs/FOAs.
- 1.2.9. Ensure completion of networkiness assessment from DISA before starting initial Operational Test and Evaluation.
- 1.2.10. Perform certification duties for the DAA in accordance with AFI 33-202.

- 1.2.11. Represent the Air Force on DMS operations working groups.
- 1.3. Headquarters Standard System Group (HQ SSG), DMS-AF PMO. HQ SSG will:
 - 1.3.1. Accomplish DMS implementation.
 - 1.3.2. Function as the Air Force registration authority (RA) for the MISSI/FORTEZZA Public Key Infrastructure (High Assurance).
 - 1.3.2.1. Provide registration and directory guidance.
 - 1.3.2.2. Define the roles of organizational registration authorities, sub-registration authorities (SRA), and certification authorities (CA).
 - 1.3.2.3. Coordinate the structure of the Air Force level of the DMS directory with AFCA, DISA, and individual Air Force sites.
 - 1.3.3. Complete sustainment actions as delegated by the DMS-AF lead command.
 - 1.3.4. Serve as the Air Force office of primary responsibility for AUTODIN phase out.
 - 1.3.5. Develop DMS-AF engineering and architecture strategies and support plans.
 - 1.3.6. Function as the single acquisition authority for Air Force requirements.
 - 1.3.7. Initiate CoN testing and provide assessment of all major software releases.
 - 1.3.8. Prepare certification and accreditation packages; submit packages to AFCA.
 - 1.3.9. Establish configuration management baseline for all software and hardware.
 - 1.3.10. Serve as Air Force focal point for all DMS detailed design changes.
 - 1.3.11. Distribute software and hardware modifications to MAJCOMs.
 - 1.3.12. Manage the deployment of certification authority workstations (CAW) at Air Force sites.
 - 1.3.13. Test the Department of Defense (DoD) computer emergency response team information assurance vulnerability alerts, Air Force time compliance network orders (TCNO), field engineering notices (FEN), and commercial fixes and configuration changes. **NOTE:** TCNOs were previously known as Air Force computer emergency response teams advisory and advisory compliance messages.
 - 1.3.14. Prepare system advisory notices for implementation on DMS components and forward to the DMS-AF Technical Support Center for distribution.
- 1.4. DMS-AF Technical Support Center (DTSC). The DTSC will:
 - 1.4.1. Operate the enterprise-level DMS-AF Help Desk (HD) to resolve problems and concerns for DMS end users and system administrators.
 - 1.4.2. Coordinate actions with and elevate problems to the DISA Regional Network Operations Center (RNOC), as required by DISA Circular (DISAC) 310-M70-87, *Operational Policies and Procedures for the Defense Message System*, and inform the appropriate MAJCOM Network Operations and Security Center (NOSC).
 - 1.4.3. Work with MAJCOM NOSCs to resolve trouble tickets escalated to the DISA RNOCs.

- 1.4.4. Advise MAJCOM NOSCs and DISA RNOCs (according to DISAC 310-M70-87) of DMS base isolation or outages and significant system degradation ([Attachment 2](#)).
- 1.4.5. Distribute SANs to MAJCOM for implementation.
- 1.4.6. Convert AUTODIN AIGs to DMS MLs and ALs.
- 1.4.7. Create MLs and ALs.
- 1.4.8. Maintain the Air Force Global Address List and Secret Internet Protocol Router (SIPRNet) Microsoft Metadirectory Services.
- 1.4.9. Maintain the Air Force Directory Service Agent (DSA) and Tactical DNS server for DMS deployed.
- 1.5. MAJCOMs, DRUs, and FOAs. MAJCOMs, DRUs, and FOAs will:
 - 1.5.1. Allocate manpower to support DMS.
 - 1.5.2. Perform CA and registration activities according to the *CAW Implementation Plan* (applicable to DRUs and FOAs that do not have a service-level agreement with base or MAJCOM).
 - 1.5.3. Provide supplemental DMS operational policies and procedures, including transitional planning guidance, message preparation, and transmission guidance.
 - 1.5.4. Provide funding for sustainment beyond program limits and acquisition of value added products, as required.
 - 1.5.4.1. Ensure system maintenance needs at the organizational level are met.
 - 1.5.4.2. Identify technology refresh, component replacement requirements, and other hardware issues to the DMS-AF PMO.
 - 1.5.5. Coordinate requirements for newly developed courses or emergency training with HQ USAF/ILCX, HQ AETC, and HQ AFCA.
 - 1.5.6. Ensure compliance with configuration control and change management processes according to DISAC 310-M70-87, and the *Air Force Change Process Guide* published by DMS-AF PMO.
 - 1.5.7. Appoint a ML manager.
 - 1.5.8. Distribute software and hardware modifications to the bases.
 - 1.5.9. Identify messaging requirements to AFCA for determination of enterprise applicability.
- 1.6. MAJCOM NOSC. **NOTE:** Also applicable to DRUs and FOAs that do not have a service-level agreement with a servicing base or NOSC. MAJCOM NOSC will:
 - 1.6.1. Provide HD services to resolve problems reported by the Network Control Center (NCC) ([Attachment 2](#)).
 - 1.6.2. Coordinate actions with and elevate problems to the Air Force Network Operations Center (AFNOC) ([Attachment 2](#)).
 - 1.6.3. Advise AFNOC of DMS base isolation or outages ([Attachment 2](#)).
 - 1.6.4. Not take action on TCNOs affecting DMS components until directed by the AFNOC.

- 1.6.5. Take action on SANs as directed by the AFNOC.
- 1.7. Installation Commander. The installation commander will:
 - 1.7.1. Provide messaging services to organizations within the area of responsibility.
 - 1.7.2. Establish local procedures for notification of MINIMIZE according to Allied Communications Publication (ACP) 121/United States Supplement (US SUP)-1, (C) *Communication Instructions General* (U).
 - 1.7.3. Enforce guidance established in ACPs, DISACs, Joint Army-Navy-Air Force publications (JANAP), Air Force (to include applicable Air Force Systems Security instructions [AFSSI]) and MAJCOM directives.
 - 1.7.4. Ensure information assurance awareness training is accomplished according to AFI 33-204, *Information Assurance Awareness Program*, and licensing and certification requirements are satisfied as required in AFI 33-115, Volume 2, *Licensing Network Users and Certifying Network Professionals*, for all users who access Air Force networks and systems.
 - 1.7.5. Determine readiness of base to close TCC.
 - 1.7.6. Appoint SRA and ML/AL cognizant authorities as needed.
 - 1.7.7. Ensure Local Control Center (LCC)-1 and base distribution point (BDP) accounts are established.
 - 1.7.8. Identify DMS training requirements to MAJCOM training manager.
 - 1.7.9. Appoint a manager of the BDP account.
 - 1.7.10. Ensure CRL are generated and posted once a week.
- 1.8. Organization Commander. Each organization commander will:
 - 1.8.1. Be responsible for all messages delivered to their organizational account to include the traffic service station (TSS) account.
 - 1.8.1.1. Establish an alternate delivery point for URGENT (High Precedence) messages when organizational accounts are not manned on a 24-hour, 7-day a week basis (24/7).
 - 1.8.1.2. Provide an after-hours notification personnel listing to the alternate delivery point of contact (POC).
 - 1.8.2. Designate release authority, as necessary.
 - 1.8.3. Refer to AFI 33-202 for granting DMS access to foreign nationals and contractors.
 - 1.8.4. Ensure DMS organizational messages are maintained according to AFMAN 37-139.
- 1.9. NCCs. NCCs will:
 - 1.9.1. Control and centrally manage network and system resources on Air Force bases or sites according to AFI 33-115, Volume 1.
 - 1.9.2. Maintain system and platform security.
 - 1.9.2.1. Not take action on TCNOs affecting DMS components until directed by the MAJCOM NOSC.

- 1.9.2.2. As directed by the MAJCOM, implement the countermeasures identified by TCNOs, advisory compliance messages, FENs, and commercial fix advisories within the timeframe specified.
- 1.9.3. Audit, record, and review DMS components' security logs periodically to determine and identify inappropriate activity according to the *DISA Defense Message System (DMS) Trusted Facility Manual*.
- 1.9.4. Prepare and update the local configuration management database when changes are made, per MAJCOM direction.
- 1.9.5. Monitor system stability and operational availability and report service interruption to DMS components and base isolation per **Attachment 2**.
- 1.9.6. Provide HD support to workgroup managers (WM).
- 1.9.7. Coordinate actions with and elevate problems to the MAJCOM NOSC (**Attachment 2**).
- 1.9.8. Follow guidance established in ACPs; DISACs; JANAPs; and Air Force, MAJCOM, and local directives.
- 1.9.9. Coordinate all DMS-AF system and equipment changes with the MAJCOM.
- 1.9.10. Perform software upgrades, as directed by the MAJCOM.
- 1.9.11. Coordinate action to decommission and remove equipment with the communications squadron plans flight, as directed.
- 1.9.12. Staff and coordinate support agreement requirements for associate units according to AFI 25-201, *Support Agreements Procedures*.
- 1.9.13. Ensure letters of agreement, memorandums of agreement, and internal procedures meet all messaging needs (e.g., alternate delivery points, after-hours notification for URGENT messages, etc.).
- 1.9.14. Establish an LCC-1 account for DMS system administration use only.
- 1.9.15. Assign trained system administrators (SA) to manage DMS components. In addition to the duties identified in AFI 33-115, Volume 1, the DMS-AF SA will:
 - 1.9.15.1. Initiate the registration process for the infrastructure components with the CA and the SRA.
 - 1.9.15.2. Request personal encrypted computer memory cards (FORTEZZA) for DMS components.
 - 1.9.15.3. Update the DMS global directory as the addresses of local DMS users change.
 - 1.9.15.4. Manage the LCC account.
- 1.9.16. Take action on SANs as directed by the DTSC.
- 1.9.17. Ensure DMS training is available for WM and end users according to AFI 33-115, Volume 1.
- 1.10. Workgroup Managers (WM). WMs will:
 - 1.10.1. Provide end-user support.

- 1.10.2. Coordinate actions with and elevate problems to the NCC ([Attachment 2](#)).
- 1.10.3. Coordinate User Agent (UA) software upgrades and modifications with the NCC and user.
- 1.10.4. Maintain documentation of UA upgrades and modifications.
- 1.11. Alternate Delivery POCs. Alternate delivery POCs will:
 - 1.11.1. Be responsible for notification of URGENT messages.
 - 1.11.2. Notify the organization commander, deputy commander, or civilian equivalent when an after-hours notification personnel listing is not on file.
- 1.12. Air Force Command and Control, Intelligence, Surveillance, and Reconnaissance Center (AFC2ISRC). The AFC2ISRC, as a DMS-AF lead command affiliate, has overall responsibility for DMS management, control, planning, and programming for the Air Force Intelligence Community (IC)/Sensitive Compartmented Information (SCI) messaging, to include tactical intelligence requirements. The AFC2ISRC will:
 - 1.12.1. Identify functional management and operational requirements for DMS-AF IC/SCI messaging to HQ AFCA.
 - 1.12.2. Maintain the DMS-AF IC/SCI technical and operational architectures.
 - 1.12.3. Create operational policy and procedures for IC/SCI messaging.
 - 1.12.4. Accomplish DMS implementation and transition for the IC/SCI community.

Section B—Defense Message System Operational Policy and Guidance

2. Policy and Guidance. ACP 121/US Sup 1; JANAP 128, *Automatic Digital Network (AUTODIN) Operating Procedures*; AFI 33-115, Volume 1; AFI 33-119, *Electronic Mail (E-Mail) Management and Use*; AFI 33-129, *Transmission of Information Via the Internet*; AFMAN 33-326, *Preparing Official Communications*; and various DISA publications contain specific policies and guidance.

2.1. Message Precedence/Grade of Service. Users will assign message precedence levels authorized on the DMS user certificate. Commanders or equivalents are the only ones authorized to release URGENT messages. Table 2.1 displays military precedence levels mapping to the DMS grades of service.

Table 1. Message Precedence/Grade of Service.

Military Precedence	DMS Grade of Service	Precedence	Speed of Service
Critic	Urgent	High	3 minutes
ECP (Y)			
Flash (Z)			
Immediate (O)	Normal	Normal	20 minutes
Priority (P)			
Routine (R)	Non-Urgent	Low	8 hours

2.2. Message Retention. Messages used to conduct Air Force business are Federal records.

- 2.2.1. Approved and released transmitted messages will be maintained in the office of record approved filing system according to AFMAN 37-139.
- 2.2.2. Messages received, whether informational or part of another business transaction or decision making process, will be maintained according to AFMAN 37-139.
- 2.3. High Precedence/Urgent After-Hours Message Notification. Notification on DMS Urgent/High-Precedence messages will be made on a 24/7 basis. Procedures for after-hours notification will be developed and implemented locally.
- 2.4. Base Distribution Point (BDP). A BDP will be created under the base locale for each site, and be able to receive signed and encrypted messages. It will be used as a default address when an organization's account or its parent unit account is not available. Use it to receive en masse distribution messages that are not specifically addressed to any organization (e.g., All Military Activities [ALMILACT]). Bases will make distribution of such messages to the necessary recipients.
- 2.5. Traffic Service Station (TSS) Account. A TSS account will be created under each organization locale to provide each organization with a DMS capability. The TSS account will be configured to receive signed and encrypted messages. The TSS account allows organizational messages to be delivered to an organization for further distribution (automated or manual). Messages sent to an organization's TSS mailbox must include distribution instructions in the body of the message.
- 2.6. LCC-1 Account. An LCC-1 account will be created and be used strictly for system administration and DMS management by the localNCC.

Section C—Messaging Centers (MC)

MCs encompass support for legacy AUTODIN messaging through the telecommunications centers and DMS in the local NCC. This section defines MC management, control, operational environment, responsibilities, basic security procedures, and several other related activities to ensure effective and efficient support for communications and information capabilities. Within the Air Force, DISA's term "LCC" and the Air Force term "NCC" are the same. For clarity, only the term "NCC" is used in this instruction.

3. Standard Practices . MC managers will:

- 3.1. Develop contingency operations plans.
- 3.2. Follow operational guidance and standards as developed in ACPs; DISACs; JANAPs; and applicable Air Force, MAJCOM, DRU, and FOA directives.
- 3.3. Maintain a master station log and dispose according to AFMAN 37-139.
- 3.4. Develop local procedures to ensure local requirements are met.
- 3.5. Set up local procedures for physical security, to include safety and fire practices, and information assurance.
- 3.6. Ensure classified documents are destroyed according to AFI 31-401, *Information Security Program Management*; and AFMAN 37-139.
- 3.7. Keep environmental conditions according to equipment specifications and set up emergency procedures for environmental equipment failures.

4. Operations Management . MC managers will:

- 4.1. Set up local procedures for alternate routing messaging traffic and timely delivery.
- 4.2. Schedule service interruptions according to DISAC 310-D70-30, *Defense Information Infrastructure (DII) Defense Message System Transition Hub (DTH) and Subscriber Operations*.
- 4.3. Ensure AIG case files remain current, to include letters or messages to users advising of deletion of AIG if not recapitulated in the appropriate time frame of 12 months according to AFMAN 33-326. Include the following information addressees in all new, modified, recapitulated, or cancelled AIGs, if they are not members of the AIG: AF ACP-AIG WASHINGTON DC, SSG MAXWELL AFB GUNTER ANNEX AL//DIGDR//, and NAVCSRF HONOLULU HI//N31DB//.
- 4.4. Send MAJCOM, DRU, or FOA requests for additions, deletions, and changes to routing indicators and PLA according to the ACP 117/CAN-US SUPP-1, *Allied Routing Indicator (RI)*, 17 March 1993. Use ACPD 38-5, *Unit Designations*, when validating proposed PLA changes to ensure accuracy of unit designations.
- 4.5. Set up local procedures for MINIMIZE (ACP 121/US Sup 1).
- 4.6. Coordinate all system and equipment changes with the communications squadron plans flight according to DISAC 310-130-1, *Submission of Telecommunications Service Requests*. Send change requests to the parent MAJCOM, DRU, or FOA, with information copies to DISA and affected DMS transition hub (DTH).
- 4.7. Limit use of AUTODIN to specific messaging services as mandated by DoD (i.e., Special Category [SPECAT]/Special Handling Designator; ACP 120, *Common Security Protocol (CSP)*, June 1998; and emergency action messages [EAM]).
- 4.8. Process all incoming messages in order of precedence on a first-in/first-out basis.
 - 4.8.1. Distribute narrative messages based on address, office symbol, or delivery instructions in the first line of text. Units not having an office symbol will provide delivery instructions to the TCC.
 - 4.8.2. Do not divulge, release, or publish the contents, purpose, effect, or meaning of messages to any person other than the addressee, the addressee's representative, or a person authorized to accept, forward, or deliver the message. *Unauthorized disclosures by military personnel violate Article 92 of the UCMJ and may result in punitive action under the UCMJ. Unauthorized disclosure by civilian personnel may result in administrative or other disciplinary action under applicable civilian personnel regulations or instructions. Violations by contractor personnel will be handled according to applicable contract law.*
 - 4.8.3. Notify the "action" addressees on receipt of IMMEDIATE and higher precedence messages. If a message management letter (MML) is not on file at the TCC, call the organization commander, deputy commander, or the appropriate representative. **NOTE:** The addressee may waive notification of IMMEDIATE message receipt, but customers must document these waivers with the TCC. Customers cannot waive notification for any message precedence above IMMEDIATE. (TCCs only)
 - 4.8.4. Notify the addressee on receipt of an emergency command precedence (ECP) message (e.g., EAM, RED ROCKET and WHITE ROCKET messages).

4.8.5. Use the base information transfer system (BITS) or the base network to deliver messages not requiring special handling. This includes routine and priority precedence messages up to and including SECRET. Do not send classified messages over unsecured networks.

4.8.6. Place messages with special handling designators, special delivery instructions, or other caveats restricting distribution in AF Form 3530, **Special or Limited Distribution Message Envelope**, at the TCC and hold for pickup. Do not send through normal delivery channels unless specifically requested by the recipient, and then only as permitted by security constraints. Release IMMEDIATE and above precedence messages, messages with special designators (such as No Foreign Nationals or Atomic Energy Restricted) and all classified messages requiring receipt, in compliance with DoD 5200.1-R, *Information Security Program*, January 17, 1997; AFPD 31-4, *Information Security*; and AFI 31-401, directly to the addressee or designated representatives.

4.8.7. Keep AF Form 3531, **Message Delivery Register**, on all messages that require a receipt.

4.8.8. Deliver TOP SECRET messages according to DoD 5200.1-R, AFPD 31-4, and AFI 31-401. Deliver TOP SECRET SPECAT messages according to the instructions for SPECAT. The person authorized to receive the SPECAT message must notify the unit's TOP-SECRET control authority of the message receipt.

4.8.9. Handle messages addressed as "PERSONAL FOR" as official Federal records. The following rules apply to PERSONAL FOR messages:

4.8.9.1. Protect the privacy of messages marked as "PERSONAL FOR." Deliver PERSONAL FOR messages to the individual named or a designated representative. Users may have their PERSONAL FOR messages delivered to a personal electronic mail (E-mail) box according to AFI 33-119.

4.8.9.2. Do not readdress.

4.8.9.3. Isolate message and hold for pickup.

4.8.9.4. Do not deliver through normal delivery channels or BITS.

4.8.9.5. Use the caveat "PERSONAL FOR (NAME)" or "PERSONAL FOR (NAME) FROM (NAME)."

4.8.9.6. Authorized for use only by general/flag officers and civilians of equivalent rank according to ACP 121/US SUP 1.

4.8.10. Isolate drug testing messages received with the phrase "DBMS EYES ONLY" (DBMS stands for Director Base Medical Services) at the end of the classification line.

4.8.11. Place Critical Nuclear Weapon Design Information (CNWDI), Cryptographic, Restricted Data, Electronic Warfare Integrated Reprogramming (EWIR), or other designators indicating special handling in the text following the security classification. Place markings for RESTRICTED DATA-ATOMIC ENERGY ACT 1954, and FORMERLY RESTRICTED DATA ATOMIC ENERGY ACT on the message as shown in DoD 5200.1-R, AFPD 31-4, and AFI 31-401.

4.8.12. Use the inspector distribution (INSPECDIS) designator within and between Air Force activities only for Inspector General activities. This flags the messages for distribution only to the office addressed and for viewing only by Inspector General personnel.

- 4.8.13. General messages addressed to customers do not require logging or retention past that of other regular message traffic. Log general messages addressed to the TCC (i.e., Joint Armed Forces publications, ALMILACT, network control message, etc.) on AF Form 3532, **General Message Record**, and file sequentially. Dispose of general messages per AFMAN 37-139, Table 33-15.
- 4.8.14. File the local office symbol address with the customer-provided list of AIG local addresses.
- 4.8.15. Keep a current list of individuals authorized to pick up and receive messages. The source document for identifying authorized users is the MML. Users should update MMLs annually, or as changes occur, whichever is sooner.
- 4.8.16. Protect information against loss or compromise.
- 4.8.17. Process outgoing messages first-in/first-out by precedence. Process high precedence messages expediently and provide status to supervisory personnel.
- 4.8.18. Assign station serial numbers manually if equipment does not automatically assign it. Use AF Form 3533, **COMMCEN Message Register**, to log originated messages, when applicable. Close out the form daily. When starting a new register, bring forward the next unused consecutive station serial number from the previous register.
- 4.8.19. Assign routing indicators, if applicable.
- 4.8.20. Proofread the entire message for proper format if prepared manually.
- 4.8.21. Verify that the table of contents (TOC) cycle redundancy check (CRC) number on the releasing document matches the internal TOC CRC on the diskette before transmission, where applicable.
- 4.8.22. Write the time of transmission if equipment does not have an automatic journal or log.
- 4.8.23. File messages sequentially by station serial number, time of file, or date-time group per local procedures.
- 4.8.24. Keep magnetic tape reels and diskettes for 72 hours and then return to originator. TCCs with automatic retrieval capability may return tapes and diskettes to the originator after processing.
- 4.8.25. The releaser's organization reproduces additional copies of outgoing messages before delivery to the TCC. Delivery to Zero Effort Network addresses is the sole responsibility of the message originator. Unless specifically directed by local policy, the TCC will not reproduce additional copies of outgoing messages for customer-related responsibilities. TCCs may self-address operational readiness inspection (ORI) exercise messages into AUTODIN to evaluate ability to manually process traffic by using the following criteria:
- 4.8.25.1. Give the affected DMS DTHs 8 hours prior notification by message of the introduction of self-addressed test message traffic.
 - 4.8.25.2. The notification message will consist of date and time of test start, approximate number of messages to send, name and telephone number of ORI POC, and name of TCC evaluated.
 - 4.8.25.3. Assign a block of station serial numbers to remote terminals to identify specific

remotes according to local instructions.

4.8.25.4. Submit high volume message inputs according to DISAC 310-D70-30.

4.8.26. Keep handling of SPECAT and other special handling messages to the minimum personnel needed to process and package the product according to governing regulations. TCC personnel must set apart the following types of messages and take the actions indicated. **NOTE:** Destroy special handling message residue (e.g., SPECAT, etc.) after transmission or return it to the originator as local conditions warrant. If returned to the originator, package and account for the material according to DoD 5200.1-R, AFPD 31-4, and AFI 31-401. Additional handling requirements are listed by category:

4.8.26.1. SPECAT Messages. Limit handling and viewing of SPECAT-designated messages to properly cleared and authorized personnel. Require direct processing of SPECAT messages between the releasing or distribution office and the TCC, or between the TCC and the addressees unless local conditions call for intermediate handling. Require special clearances and access for personnel at such intermediate points to handle the SPECAT material. Activities that need to send or receive SPECAT messages give the servicing TCC a special access list of personnel who may sign for SPECAT messages. Follow the SPECAT designator with "EXCLUSIVE FOR (NAME)" or by a specific identification, acronym, or code word identifying the project or subject. Refer to ACP 121/US SUP 1F for further guidance. Types of SPECAT messages:

4.8.26.1.1. EXCLUSIVE FOR. Example: S E C R E T SPECAT EXCLUSIVE FOR GEN SMITH. **NOTE:** Do not use terms or phrases such as "EYES ONLY," "PERSONAL FOR," etc., on SPECAT messages.

4.8.26.1.2. Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI) governed by AFI 10-1102, *Safeguarding the Single Integrated Operational Plan (SIOP)*. Example: TOP SECRET SPECAT SIOP-ESI.

4.8.26.2. Special Handling Messages. Establish procedures for messages requiring special handling (e.g., CRITIC, ECP, EAM, FLASH, RED and WHITE ROCKET, TOP SECRET, PERSONAL FOR, EWIR, CNWDI, INSPECDIS, and Drug Testing).

4.8.26.2.1. Process these messages with minimal pre-logging. Fill in logs after transmission.

4.8.26.2.2. Advise the originator of delays or anticipated delays in message processing.

4.8.26.2.3. Other special handling message requirements:

4.8.26.2.3.1. EWIR. Do not retain the media used for transmission or associated printouts for more than 3 days after transmission. Return all products to the originator on completion of service action or retransmission requests.

4.8.27. Scan all diskettes for viruses.

4.8.28. Local Area Networks (LAN). LANs are authorized for record message distribution. The TCC operator will:

4.8.28.1. Establish profiles to identify and distribute messages through key word searches.

4.8.28.2. Distribute messages with special handling designators, special delivery instructions,

or other caveats restricting distribution provided the system operating software is able to limit access to authorized personnel.

4.8.29. Message Preparation Errors. The TCC operator will:

4.8.29.1. Follow local procedures for contacting releasing officials or complete a Department of Defense (DD) Form 1503, **Message Correction Notice**, on messages that contain major errors that require correction prior to transmission.

4.8.29.2. Coordinate with the releasing official or message drafter to resolve minor preparation errors that do not preclude processing and transmitting the message.

4.8.30. Use service messages for exchanging information and to correct, clarify, report, or ease the flow of message traffic. Also, use them to make notification of anticipated workloads of an unusual nature, SPECAT information, or information requiring special handling, the adjustment of procedural discrepancies, or changes to available facilities. Only use authorized and appropriate operating signals and short text instructions for service messages. Refer to ACP 127/US SUP 1, *Communications Instructions Tape Relay Procedures*, November 1998; ACP 131, *Communications Instructions Operating Signals*, March 1997; and JANAP 128 for further guidance.

5. Message Distribution Terminal (MDT) Operations . Use the MDT as the control station for its remote tributary stations. MDT personnel will:

5.1. Protect information against loss or compromise.

5.2. Follow security practices.

5.3. Follow communications security (COMSEC) procedures as found in AFI 33-201, *Communications Security (COMSEC) (FOUO)*, and AFKAG-1, *Air Force Communications Security (COMSEC) Operations (FOUO)*.

5.4. Assist the TCC in obtaining unique routing indicators.

5.5. Furnish the TCC with copies of current AIGs used to transmit or receive messages.

5.6. Publish and coordinate local procedures with the MDT to cover the processing of service messages by those remotes manned by Air Force specialty code (AFSC) 3C0X1 personnel. The host MDT personnel take care of all service actions for remotes manned by non-AFSC 3C0X1 personnel.

5.7. Set up a formal system of network control messages.

5.8. Give technical assistance and training.

5.9. Maintain system control to minimize operational impact of failures to tributaries, the MDT, or the connected DTH.

5.10. Set up and keep a workable alternate routing plan to protect tributary stations from loss or excessive delay of information during equipment or circuit outages.

5.11. Develop and maintain a customer education package for distribution to all customer-operated terminals.

5.12. Keep a continuity folder with system configurations, crossfeed information from HQ SSG, and appropriate reference materials and operating instructions.

5.13. Configure the MDTs to access the DMS Message Conversion System (MCS) Central Directory Component, the authoritative source for AUTODIN PLAs.

6. Storage Media Management . MC managers will:

- 6.1. Set up procedures that cover control, security, and upkeep of all storage media.
- 6.2. Label magnetic media as prescribed in DISAC 310-70-30 and DoD 5200.1-R.
- 6.3. Clear magnetic media with classified or personal information and remove any labels or documentation attached that could reveal the previous contents of the cleared magnetic media or its sensitivity according to AFSSI 5020 (will become AFMAN 33-224).
- 6.4. Maintain and use magnetic media, if required, according to local instructions.
- 6.5. Mark, ship, and safeguard classified magnetic media according to DoD 5200.1-R and AFI 31-401.
- 6.6. Perform system backups from the system internal storage to an external storage device. Backup frequency requirements are site specific, but recommend as a minimum:
 - 6.6.1. Accomplish a daily incremental backup.
 - 6.6.2. Accomplish a full backup weekly.
- 6.7. Store weekly full backups in an area physically separated from the MC.
 - 6.7.1. Select the off-site storage location based on its proximity to the MC, the temperature and humidity, and the physical security of the building.
 - 6.7.2. Rotate/Replace old weekly full backups with the most current weekly backup.
 - 6.7.3. Back up and store critical system programs, system software routines, and production programs in the off-site storage location.
- 6.8. Establish and maintain a magnetic media cleaning or rehabilitation cycle.
 - 6.8.1. Keep a record, by reel, pack, or cartridge number, of the date serviced.
 - 6.8.2. Turn in items no longer usable to the local Defense Property Disposal Agency according to DoD 4160.21-M, *Defense Reutilization and Marketing Manual*, August 18, 1997.
- 6.9. Maintain library records that provide listings of the media on hand in the library, those temporarily out for cleaning or rehabilitation, magnetic media shipped out for use elsewhere, those on hand belonging to another center or organization, and any media awaiting disposition.
- 6.10. Control and inventory classified magnetic media in the library as prescribed in DoD 5200.1-R and AFI 31-401.

7. Facility Management . MC managers will:

- 7.1. Set up local procedures for physical security and information protection.
- 7.2. Set up safety and fire practices.

- 7.3. Keep environmental conditions according to equipment specifications and set up emergency procedures for environmental equipment failures. Facilities that have an energy management control system do not require recording devices.
- 7.4. Make sure equipment rooms are kept clean.
- 7.5. Develop contingency operations plans.
- 7.6. Establish a preventive maintenance schedule for all equipment.
- 7.7. Make procedures for operating computer equipment during severe weather conditions such as thunderstorms within 10 statute miles of an installation, ice storms, high wind conditions, etc.

8. Automatic Digital Network Plain Language Address and Address Indicator Group Transition in Defense Message System . Overall responsibilities are as follows:

- 8.1. PLA/AIG Managers. PLA/AIG managers will list all PLAs and AIGs in the Master Update Authority (name changed from Naval Common Source Routing File). PLAs updated in the Master Update Authority database are replicated in the Defense Information Infrastructure (DII) Asset Distribution System database.
- 8.2. Cognizant Authorities. The cognizant authorities will forward all PLA additions, changes, and deletions according to ACP 117/CAN-US SUPP 1K (to include page number, action to be taken, location for each entry, the unit/agency, and routing indicator [RI]) to their respective MAJCOM representative.
- 8.3. MAJCOM PLA Representative. The MAJCOM PLA representative will:
 - 8.3.1. Review and validate the PLA changes.
 - 8.3.2. Forward the change requests to the Mission Systems Branch (HQ USAF/ILCSM) (AF ACP-AIG WASHINGTON DC).
- 8.4. Mission Systems Branch (HQ USAF/ILCSM) (AF ACP-AIG WASHINGTON DC). HQ USAF/ILCSM will approve all PLAs additions, deletions, and submit changes to the Master Update Authority.

9. Addresses .

- 9.1. HQ USAF/ILCSM, 1030 Air Force Pentagon, Washington DC 20330-1030.
- 9.2. HQ AFCA/GCOM, 203 West Losey Street, Scott AFB IL 62225-5222.
- 9.3. HQ SSG/DIGD, 501 East Moore Drive, Maxwell AFB-Gunter Annex AL 36114-3312.
 - 9.3.1. HQ SSG/SWSND, 401 East Moore Dr. Maxwell AFB-Gunter Annex AL 36114-3001.

10. Information Collections, Records, and Forms or Information Management Tool (IMT) .

- 10.1. Information Collections. Information collections created by this publication are exempt from licensing in accordance with paragraph 2.11.10 of AFI 33-324.
- 10.2. Records. Records pertaining to messaging are created by this publication (paragraphs [2.4.](#), [3.2.](#), [4.8.7.](#), [4.8.13.](#), [4.8.15.](#), [4.8.18.](#), and 4.8.32). Retain and dispose of messaging records according AFMAN 37-139, Table 33-8 and table 33-15, Rule 13.

10.3. Forms or IMTs (Adopted and Prescribed).

10.3.1. Adopted Forms or IMTs. DD Form 1503, **Message Correction Notice**, and AF Form 847, **Recommendation for Change of Publication**.

10.3.2. Prescribed Forms or IMTs. The following Air Force forms are prescribed by this publication: AF Form 3530, **Special or Limited Distribution Message Envelope**, AF Form 3531, **Message Delivery Register**; AF Form 3532, **General Message Record**; AF Form 3533, **COMMCEN Message Register**.

MICHAEL E. ZETTLER, Lt Gen, USAF
DCS/Installations and Logistics

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

Paperwork Reduction Act of 1974 as amended in 1996

ACP 117/CAN-US SUPP-1, *Allied Routing Indicator (RI)*

ACP 120, *Common Security Protocol*

ACP 121/US SUP 1, (C) *Communication Instructions General (U)*

ACP 127/US SUP 1, *Communications Instructions Tape Relay Procedures*

ACP 131, *Communications Instructions Operating Signals*

JANAP 128, *Automatic Digital Network (AUTODIN) Operating Procedures*

DoD 4160.21-M, *Defense Reutilization and Marketing Manual*, August 18, 1997

DoD 5200.1-R, *Information Security Program*, January 17, 1997

DISA *Defense Message System (DMS) Trusted Facility Manual*, DMS Release 2.2, December 1, 2000

DISAC 310-D70-30, *Defense Information Infrastructure (DII) Defense Message System Transition Hub (DTH) and Subscriber Operations*.

DISAC 310-M70-87, *Operational Policies and Procedures for the Defense Message System*

DISAC 310-130-1, *Submission of Telecommunications Service Requests*

Uniform Code of Military Justice

AFPD 31-4, *Information Security*

AFPD 33-1, *Command, Control, Communications, and Computer (C4) Systems*

AFPD 38-5, *Unit Designations*

AFI 10-901, *Lead Operating Command--Communications and Information Systems Management*

AFI 10-1102, *Safeguarding the Single Integrated Operational Plan (SIOP)*

AFI 25-201, *Support Agreements Procedures*

AFI 31-401, *Information Security Program Management*

AFI 33-115, Volume 1, *Network Management*

AFI 33-115, Volume 2, *Licensing Network Users and Certifying Network Professionals*

AFI 33-119, *Electronic Mail (E-Mail) Management and Use*

AFI 33-129, *Transmission of Information Via the Internet*

AFI 33-201, *Communications Security (COMSEC) (FOUO)*

AFI 33-202, *Computer Security*

AFI 33-204, *Information Assurance (IA) Awareness Program*

AFI 33-324, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections*

AFMAN 33-326, *Preparing Official Communications*

AFMAN 33-360, Volume 2, *Forms Management Program*

AFMAN 37-139, *Records Disposition Schedule*

AFSSI 5020, *Remanence Security* (will become AFMAN 33-224)

AFKAG-1, *Air Force Communications Security (COMSEC) Operations* (FOUO)

Air Force Change Process Guide

CAW Implementation Plan

Abbreviations and Acronyms

AFC2ISRC—Air Force Command and Control, Intelligence, Surveillance, and Reconnaissance Center

ACP—Allied Communications Publication

AETC—Air Education and Training Command

AF—Air Force (used on forms only)

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFNOC—Air Force Network Operations Center

AFPD—Air Force Policy Directive

AFSC—Air Force Specialty Code

AFSSI—Air Force Systems Security Instruction

AIG—Address Indicator Group

AL—Address List

ALMILACT—All Military Activities

ASI—Authorized Service Interruption

AUTODIN—Automatic Digital Network

BDP—Base Distribution Point

BITS—Base Information Transfer System

CA—Certification Authority

CAW—Certification Authority Workstation

CNWDI—Critical Nuclear Weapon Design Information

COMSEC—Communications Security

CoN—Certificate of Networkiness

CRC—Cycle Redundancy Check
CRL—Certificate Revocation List
DAA—Designated Approving Authority
DBMS—Director Base Medical Services
DD—Department of Defense (used on forms only)
DII—Defense Information Infrastructure
DISA—Defense Information Systems Agency
DISAC—Defense Information Systems Agency Circular
DMS—Defense Message System
DMS-AF—Defense Message System-Air Force
DoD—Department of Defense
DRU—Direct Reporting Unit
DSA—Directory Service Agent
DTH—DMS Transition Hub
DTSC—DMS-AF Technical Support Center
E-mail—Electronic Mail
EAM—Emergency Action Message
ECP—Emergency Command Precedence
EWIR—Electronic Warfare Integrated Reprogramming
FEN—Field Engineering Notice
FOA—Field Operating Agency
HD—Help Desk
HQ AFCA—Headquarters Air Force Communications Agency
HQ SSG—Headquarters Standard Systems Group
HQ USAF—Headquarters United States Air Force
IC—Intelligence Community
IMT—Information Management Tool
INSPECDIS—Inspector Distribution
ITU-T—International Telecommunication Union-Telecommunication Standardization Sector
JANAP—Joint Army-Navy-Air Force Publication
LAN—Local Area Network
LCC—Local Control Center

MAJCOM—Major Command
MC—Messaging Center
MCS—Message Conversion System
MDT—Message Distribution Terminal
ML—Mail List
MLA—Mail List Agent
MTA—Message Transfer Agent
MML—Message Management Letter
NAVCSRF—Naval Common Source Routing File
NCC—Network Control Center
NOSC—Network Operations and Security Center
ORI—Operational Readiness Inspection
PLA—Plain Language Address
PMO—Program Management Office
POC—Point of Contact
RA—Registration Authority
RI—Routing Indicator
RNOC—Regional Network Operations Center
SA—System Administrator
SCI—Sensitive Compartmented Information
SHD—Special Handling Designator
SIOP-ESI—Single Integrated Operational Plan-Extremely Sensitive Information
SPECAT—Special Category
SRA—Sub-Registration Authority
24/7—24 Hours a Day/7 Days a Week
TCC—Telecommunications Center
TCNO—Time Compliance Network Order
TOC—Table of Contents
TSS—Traffic Service Station
UA—User Agent
UCMJ—Uniform Code of Military Justice
US SUP—United States Supplement

WM—Workgroup Manager

Terms

Address List (AL)—A single message address that acts as a collective address. Address Lists use a V3 certificate and are centrally managed at the ML Support Center. Each AL has a cognizant authority, a control authority, a manager, members, and permitted users. ALs are created from AUTODIN AIGs and V1 DMS Mail Lists and will use the same number designator (e.g., AIG 123 and ML 123 will become AL 123).

Air Force Network Operations Center (AFNOC)—The Air Force's top network management tier. This top-tier organization provides senior leaders the network enterprise view across the Air Force. One of its primary roles is to manage base-level Service Delivery Points Non-Secure Internet Protocol Router Network/Secret Internet Protocol Router Network routers to produce global visibility of the Air Force's enterprise network. The AFNOC monitors and responds to anomalies in communications and information networks, systems, and applications through interactions with the DISA, MAJCOMs, and commercial sector.

Architecture of Defense Message System—The structure and inter-relationship of DMS components and the principles and guidelines governing the design and evolution over time.

Certification Authority (CA)—The person responsible for user certification and programming of FORTEZZA cards. The CA generates FORTEZZA cards using the CAW.

Certification Authority Workstation (CAW)—A trusted workstation that is used only by the CA. The CA software runs on a trusted workstation with two FORTEZZA card readers, one of which is used for the CA's card and the other for the card being programmed for the user.

Clearing—Removal of data from a communications and information system, its storage devices, and other peripheral devices with storage capacity in such a way that the data may not be reconstructed using common system capabilities.

Component—A software process and its hardware platform that perform a service in the preparation, transmission, or translation of messages (i.e., user client, groupware server, message transfer agent [MTA], directory system agent [DSA], integrated directory user agent, administrative directory user agent, certification authority workstation [CAW], mail list agent [MLA], management workstation, multi-function interpreter).

Directory—A collection of open systems cooperating to provide directory service. As used in this document, it refers specifically to the DMS directory, based on the International Telecommunication Union-Telecommunication Standardization Sector (ITU-T) X.500 recommendations.

Directory Information Tree—A directory information base that employs a flat tree structure.

Directory Service—A service of the external environment entity of the technical reference model. It provides locator services that are restricted to finding the location of a service, location of data, or translation of a common name into a network specific address. It is analogous to a telephone book and supports distributed directory implementations.

FORTEZZA—The name given to the Personal Computer Memory Card International Association card used in the encryption and authentication of DMS messages.

Help Desk (HD)—The primary POC for reporting system problems, reporting transport network

problems, and requesting technical assistance. The HD also provides inquiry and informational support in the areas of component setup and system administration, coordination of site preparation and implementation, and component approval. A HD is located at each regional operations and security center and network control center.

Isolation—A site or group of DMS users that has lost connectivity with the rest of the DMS community through the DMS backbone.

Local Control Center (LCC)—Synonymous to network control center. The facility at a base, camp, post, or station that provides technical control and monitors the system at the local level.

Mail List (ML)—A single message address that acts as a collective address. Mail Lists use a V1 certificate and are centrally managed at the ML Support Center by the DMS-AF PMO. Each ML has a cognizant authority, a control authority, a manager, members, and permitted users. Refer to the mail list concept of operations for responsibilities of each player and details on procedures. MLs are created from AUTODIN AIGs and will use the same number designator (e.g., AIG 123 will become ML 123).

Mail List Agent (MLA)—A DMS component that accepts messages addressed to MLs and readdresses the messages to the individual recipients who are members of the ML.

Messaging Center (MC)—Messaging Centers provide messaging support for legacy Automatic Digital Network (AUTODIN) through the local telecommunications centers (TCC), and the Defense Message System (DMS) in the local Network Control Center (NCC).

Network Operations and Security Center (NOSC)—The NOSC is the conduit between the AFNOC and the NCC. It provides commanders visibility into the network to achieve operational objectives. The NOSC exercises command and control over its networks and mission systems. The NOSC performs MAJCOM enterprise management, helps achieve information assurance, and provides MAJCOM network visibility for timely situational awareness.

Organizational Message—A message exchanged between organizational elements.

Outage—Any denial or significant impairment of DMS messaging, specialty product, or directory service to one or more DMS user as a result of a DMS site, DMS component, or DMS supporting component failure. Outages may be scheduled or unscheduled.

“PERSONAL FOR” Message—A special message delivery instruction used to identify a specific individual or position title to whom a message is to be delivered.

Plain Language Address (PLA)—The standard military message address of an organization in the JANAP 128 format.

Regional Network Operations Center (RNOC)—The facility in a region that provides technical control and monitors the system at the regional level.

Registration Authority (RA)—A person or organization having authority over a portion of the directory information tree.

Subordinate Message Transfer Agent—A message transfer agent occupying, in the DMS hierarchical architecture, the lowest level, and serving a local area or community.

Sub-Registration Authority (SRA)—The SRA assigns directory distinguished names, is responsible for registration matters, and maintains the DMS directory at the local level.

User Agent (UA)—As defined in ITU-T X.400, a software component of the message handling system

through which a single direct user engages in message handling. The UA assists users in the preparation, storage, and display of messages.

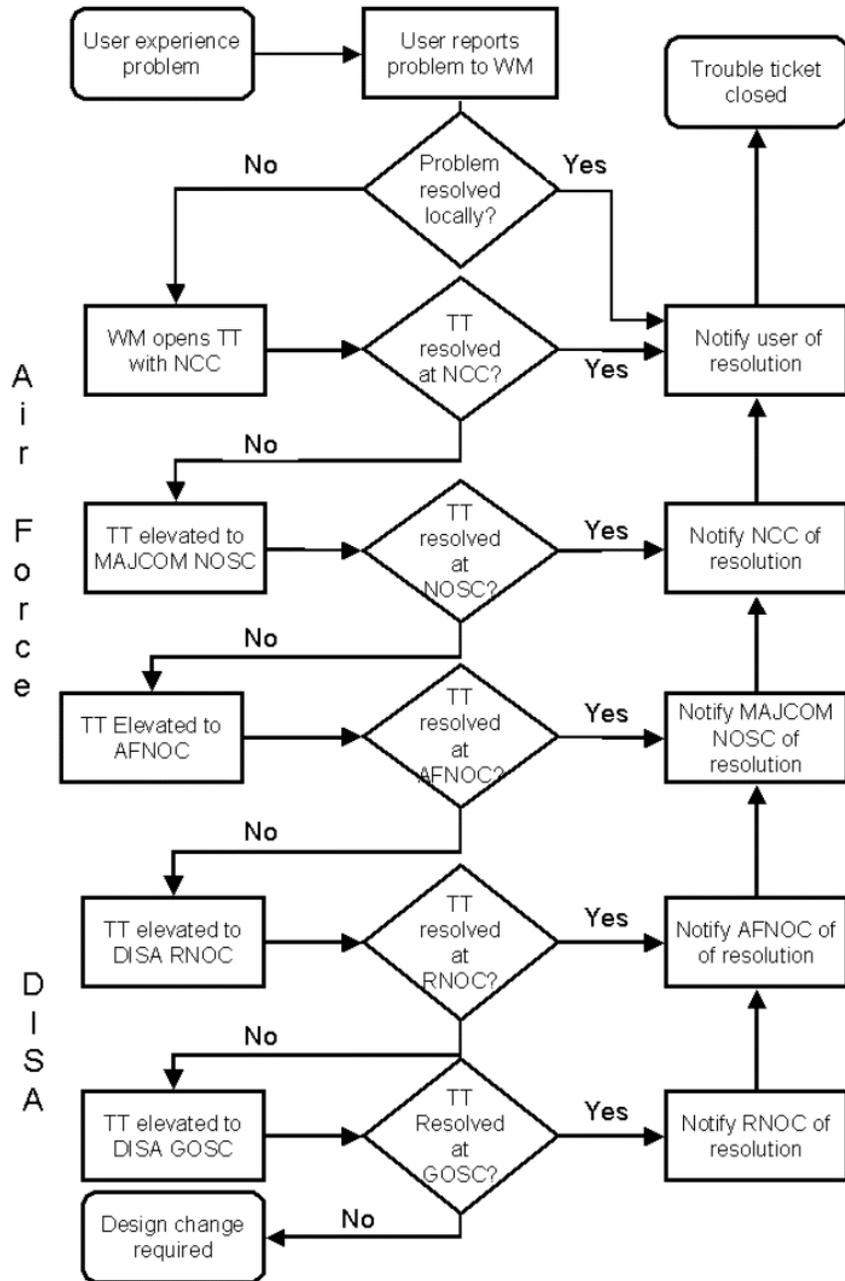
Value-Added Products—Products that are not on the Core Product List that are necessary to satisfy Air Force-unique operational electronic messaging and directory requirements. Products connected to the DMS components must undergo testing before being approved for implementation. A Value-Added Products Working Group will determine the level of testing required.

Attachment 2

DEFENSE MESSAGE SYSTEM TROUBLE & OUTAGE REPORTING

A2.1. Defense Message System Trouble Reporting. Figure A2.1. identifies the trouble reporting and resolution reporting process for scheduled and unscheduled outages, site isolations, and site status.

Figure A2.1. Trouble Reporting and Resolution Process.



A2.2. Defense Message System Outage Reporting . An outage is any denial or significant impairment of DMS messaging or directory services as a result of a DMS site, DMS component, or a DMS supporting component failure. Priority 1, 2, and 3 outages, lasting more than the duration identified in **Table A2.1.**, will be reported. NCCs report outages to the MAJCOM NOSC; the MAJCOM NOSC reports the outage to the DISA NOCs. Bases/MAJCOMs will determine reporting time requirements for Priority 4 Authorized Service Interruptions (ASI) reporting.

A2.2.1. Outages will be reported using the Air Force-approved trouble ticket system. Each outage will have a trouble ticket assigned to it. If it is not possible to initiate a trouble ticket, outages will be reported by one of the following methods, in order of elimination:

A2.2.1.1. DMS Message or Medium Grade Service (MGS) Message.

A2.2.1.2. Phone.

A2.2.1.3. Simple Mail Transfer Protocol E-mail.

A2.2.1.4. Facsimile.

NOTE: Follow up all electronic transmission outages with a phone call.

Table A2.1. DMS Outage Duration Reporting Criteria.

Site Status	Priority	Description	Duration of Outage
Red	1	Site Isolation (Major Mission Impact). An isolation occurs when a site or group of DMS users have lost connectivity with the rest of the DMS community through the DMS backbone.	10 Minutes
Amber	2	Component outage (Possible Mission Impact). Any component outage to include any infrastructure (local message transfer agent, local directory system agent, MLA, etc.) and any DMS supporting component (DTH/MCS, CAW, LAN, etc.). Site operating without backup components.	30 Minutes
Green	3	Limited Outage (No mission impact). Any other denial or significant impairment of DMS messaging, or directory services to more than one user but does not isolate a unit or base.	8 Hours
ASI	4	Scheduled Authorized Service Interruption (Minimal Mission Impact). Any DMS outage scheduled in advance. May be reported as an outage at the time of the service interruption.	As needed or determined by DMS system administrator or network control center leadership