BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-113

1 MARCH 1998

Communications and Information

MANAGING MESSAGING AND DATA PROCESSING CENTERS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the SAF/AAD WWW site at: http://afpubs.hq.af.mil. If you lack access, contact your Publishing Distribution Office (PDO).

OPR: HQ AFCA/GCOM (SMSgt Coari)
Supersedes AFI 33-113, 1 April 1996.

Certified by: HQ USAF/SCXX (Lt Col Webb)
Pages: 47
Distribution: F

This instruction implements Air Force Policy Directive (AFPD) 33-1, *Command, Control, Communications and Computer (C4) Systems*. This instruction provides procedures and assigns responsibilities for managing messaging centers (MC) and data processing centers (DPC). MCs encompass legacy telecommunications centers (TCC), Defense Message System (DMS), and local control center (LCC) functions of Air Force network control centers (NCC). It outlines the Air Force strategy to operate and manage messaging support for Air Force bases worldwide and defines MC and DPC 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, the Defense Information Systems Agency (DISA) term LCC and the Air Force term NCC are one and the same. Within this document, we only use the term NCC. Refer technical questions about this instruction to Headquarters Air Force Communications Agency (HQ AFCA/GCOM), 203 West Losey Street, Room 3065, Scott AFB IL 62225-5233. Refer recommended changes and conflicts between this and other publications on AF Form 847, **Recommendation for Change of Publication**, through channels, to HQ AFCA/XPXP, 203 West Losey Street, Room 1060, Scott AFB IL 62225-5233. **Violations of the prohibitions of paragraphs 1.7.2 and 7.1.3 by military members constitutes a violation of Article 92, Uniform Code of Military Justice (UCMJ), and may result in punishment under the UCMJ. Violations of paragraph 7.1.3 by civilian personnel may result in administrative or other disciplinary action under applicable civilian personnel regulations or instructions.** See **Attachment 1** for a glossary of terms and supporting information.

SUMMARY OF REVISIONS

This document was substantially revised and must be completely reviewed. It eliminates operational requirements for the retired automated message processing exchange (AMPE) system; eliminates the limited distribution (LIMDIS) special handling designator; establishes DMS operational policies and procedures, including security requirements and mail list management; defines new DMS terms, abbreviations, and acronyms; and identifies DMS hierarchy organizational roles and responsibilities. It adds **Attachment 5** to help users develop a checklist that manages taskings imposed by this publication. You may use

AF Form 2519, **All Purpose Checklist**, as a tool to create the checklist. It makes AF Form 3534, **Channel Number Sheet**, obsolete.

Section A—Roles and Responsibilities

1. Roles and Responsibilities:

1.1. DMS-AF Manager. The DMS-AF manager is located at Headquarters Air Force Communications and Information Center (HQ AFCIC/SYNT). HQ AFCIC/SYNT has overall responsibility for the management, control, planning, and programming of DMS. The DMS-AF manager will:

1.1.1. Execute and manage the planning, programming, budgeting, and implementation activities of the DMS.

1.1.2. Develop acquisition, fielding, and support plans and strategies.

1.1.3. Ensure test and evaluation activities support DMS migration to an open system.

1.1.4. Function as the Air Force control authority for mail lists (ML).

1.2. HQ AFCA. HQ AFCA, as lead command for DMS-AF, according to AFI 10-901, *Lead Command-Communications and Information Systems Management*, creates operations and information protect policy and guidance. HQ AFCA responsibilities include:

1.2.1. Management and requirements processing.

1.2.2. Operational policies and procedures.

1.2.3. Training.

1.2.4. Manpower.

1.2.5. Deployment.

1.2.6. Security.

1.2.7. Message preparation and transmission guidance.

1.2.8. Air Force approving authority (AA).

1.2.9. Appointing certification authorities (CA).

1.2.10. Air Force office of primary responsibility (OPR) for ML and address indicator group (AIG) management, administration policy, and procedures.

1.3. HQ Standard Systems Group (SSG). HQ SSG is the DMS-AF Program Management Office (PMO) and is responsible for:

1.3.1. DMS implementation.

1.3.2. Air Force registration authority (RA).

1.3.3. Registration and directory guidance.

1.3.4. Sustainment.

1.3.5. Automatic Digital Network (AUTODIN) phase-out.

1.3.6. Engineering and architecture.

1.3.7. Single acquisition authority for Air Force requirements.

1.4. Major Commands (MAJCOM), Direct Reporting Units (DRU), and Field Operating Agencies (FOA). These organizations will:

1.4.1. Provide manpower for operational facilities.

1.4.2. Provide local operational policies and procedures, including transitional planning.

1.4.3. Ensure communications and information processing equipment and personnel meet the needs of the users.

1.4.4. Provide funding beyond DMS-AF PMO and DISA limits.

1.4.5. Establish traffic analysis standards or other measurements to evaluate performance according to local procedures. Send copies of MAJCOM/DRU/FOA-developed standards to HQ AFCIC/SYNT and HQ AFCA/GCOM for consideration in developing Air Force standards.

1.4.6. Ensure information protection (IP) requirements stated in this AFI are included in the MAJCOM program.

1.5. Messaging Centers. NCCs are responsible for all of the customer service; first-look, line replaceable unit (LRU) maintenance of user level components (user agents [UA], personal computer memory card international association [PCMCIA] reader, profiling user agents [PUA]). The NCC also monitors and controls intermediate and subordinate message transfer agents (MTA), multi-function interpreters (MFI), directory system agents (DSA), PUAs, and UAs. MCs will:

1.5.1. Maintain system and platform security.

1.5.2. Configure and audit security logs for DMS components *(NCCs only)*.

1.5.3. Prepare and update the local configuration management database per information from users.

1.5.4. Monitor traffic loads at the local level and take action to correct problems.

1.5.5. Act as a focal point for system level operations affecting its main site and connecting sub-sites.

1.5.6. Coordinate actions with, and elevate problems to, the Regional Operations and Security Center (ROSC) as required *(NCCs only)*.

1.5.7. Provide help desk service (customer service) to resolve user problems and concerns.

1.5.8. Follow guidance and standards already established in allied communications publications (ACP); DISA circulars (DISAC), Joint Army-Navy-Air Force publications (JANAP), and MAJCOM, DRU, and FOA directives.

1.5.9. Establish local alternate routing procedures to ensure high priority users have the capability of establishing associations with at least two subordinate message transfer agents (SMTA).

1.5.10. Coordinate base connectivity interruptions to the DMS infrastructure with the servicing ROSC *(NCCs only)*.

1.5.11. Maintain a station log to record significant events.

1.5.12. Establish local procedures for notification of MINIMIZE.

1.5.13. Perform measurements and traffic analysis to evaluate system and component performance according to established standards.

1.5.14. Coordinate all DMS system and equipment changes with the DMS-AF PMO and DISA *(NCCs only)*.

1.5.15. Ensure authorized personnel pick-up output products or send them through the base information transfer system (BITS) as security requirements permit.

1.5.16. Decommission and remove equipment, through the plans flight, when no longer needed.

1.5.17. Maintain an on-the-job training program.

1.5.18. Establish a customer education program.

1.5.19. Ensure destruction facilities meet the needs of the MC and DPC.

1.5.20. Staff and coordinate support agreement requirements for all tenants (AFI 25-201, *Support Agreement Procedures*), through the plans flight.

1.5.21. Ensure letters of agreement, memorandums of agreement, and internal procedures exist with OPRs to meet all messaging needs (e.g., alternate delivery points, after hours notification, etc.).

1.5.22. Appoint sub-registration authorities (SRA), organizational registration authorities (ORA), and ML CAs *(NCCs only)*.

1.5.23. Perform fault management functional duties *(NCCs only)*.

1.5.24. Appoint an immediate access storage manager for each installed computer system *(NCCs only)*.

1.6. DMS System Administrators (SA). The NCC will assign a SA for each DMS component the NCC maintains. These SAs are part of the technical cadre of personnel assigned to the NCC and are responsible for a DMS host or platform. This includes the operating system and system configuration, the loaded applications, system backup and recovery security protection, and its local area network (LAN) network connectivity. While the NCC may delegate some responsibilities (such as component backup) for decentralized components to non-NCC personnel, overall SA responsibilities remain with the NCC. The NCC SA will also:

1.6.1. Prepare standard operating procedures (SOP) for the administration and use of the various regional level components within the area of responsibility (AOR).

1.6.2. Initiate the registration process for the infrastructure components with the CA and the SRA.

1.6.3. Establish an infrastructure for registering each component with adjacent components to allow proper authentication and for distributing the means of authentication (i.e., passwords, etc.).

1.6.4. Request personal encrypted computer memory cards (FORTEZZA) for DMS components.

1.6.5. Analyze problems or assist local or regional DMS analysts in doing so.

1.6.6. Oversee or perform the installation of new hardware and software upgrades.

1.6.7. Perform system backups and recoveries on components.

1.6.8. Perform system configuration including boot start-up and shut-down processes.

1.6.9. Perform archive and delete functions of the audit log as recommended by the computer systems security officer (CSSO).

1.6.10. Perform reconfiguration of components.

1.6.11. Assist the CSSO as required by Air Force Systems Security Instruction (AFSSI) 6001, *Operational Instruction for Components and Systems Supporting the Multilevel Information Systems Security Initiative (MISSI)* as required by the IP program according to AFPD 33-2, *Information Protection*.

1.6.12. Maintain the local part of the global directory that will be updated as the location of DMS users changes.

1.6.13. Perform configuration management duties and responsibilities.

1.7. Messaging Users. Users will:

1.7.1. Comply with operating procedures and supplements.

1.7.2. Safeguard both FORTEZZA card and personal identification number (PIN). **Failure to properly safeguard the FORTEZZA card or unauthorized disclosure of a PIN violates Article 92 of the UCMJ and may result in administrative or disciplinary action.**

1.7.3. Ensure messages transmitted are given the proper security level and precedence.

1.7.4. Report problems to the functional workgroup manager (WGM). The WGM will then determine the level of escalation required to solve the problem.

1.7.5. Limit directory searches as defined by local policy.

1.7.6. Comply with communications security (COMSEC) and computer security (COMPUSEC) requirements.

1.7.7. Safeguard messages and information protected under the Privacy Act.

1.7.8. Establish internal procedures to control and prevent tampering of transmitted and received messages.

Section B—Facility Management

2. Facility Management. MC and DPC managers will:

2.1. Set up local procedures for physical security and IP.

2.2. Set up safety and fire practices.

2.3. 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.

2.4. Make sure MC and DPC equipment rooms are kept clean.

2.5. Develop contingency operations plans.

2.6. Establish a preventive maintenance (PM) schedule for all equipment. Develop a written agreement for contractor-maintained equipment. See **Attachment 3** for a sample memorandum to use with contractor-maintained equipment.

Section C—Messaging Center and Data Processing Center Operations Management

3. Operations Management. MC and DPC managers will:

3.1. Follow guidance and standards as developed in ACPs, DISACs, JANAPs, and Air Force, MAJCOM, DRU, FOA, and other applicable directives.

3.2. 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.) including contractual liabilities for unique systems.

3.3. Set up local procedures for alternate routing of messaging traffic.

3.4. Schedule AUTODIN service interruptions according to DISAC 310-70-30, *DCS AUTODIN Switching Center and Subscriber Operations*.

3.5. Maintain a station log.

3.6. Make sure AUTODIN AIG and DMS ML case files remain current at all times, to include letters or messages to users advising them of deletion of their AIG or ML if not recapitulated in the appropriate time frame of 12 months according to Air Force Manual (AFMAN) 37-126, *Preparing Official Correspondence* (to become AFMAN 33-326). Include NAVCSRF HONOLULU HI//N33// and AF ACP-AIG WASHINGTON DC// as information addressees in all new, modified, or canceled AIGs, if they are not members of the AIG.

3.7. Send your MAJCOM, DRU, or FOA requests for additions, deletions, and changes to routing indicators and plain language addresses (PLA) in all ACP 117s. They use AFPD 38-5, *Unit Designations,* when validating proposed plain language address changes to make sure of uniformity of unit designations.

3.8. Set up local procedures for MINIMIZE (ACP 121 USSUP1(), [C] *Communications Instructions-General [U]*).

3.9. Coordinate all AUTODIN system and equipment changes with the communications unit planning and implementation activity 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 AUTODIN switching centers (ASC).

3.10. Use software deficiency reports to identify problems preventing the system from performing its designed functions (see **Attachment 4**). Deficiency reports fall into the following categories:

3.10.1. Emergency Deficiency Reports (Category 1) for problems that result from system failures, security hazards, loss or duplication of data, or other conditions that seriously impact data handling.

3.10.1.1. TCCs will notify the applicable software support office via telephone. Follow up with a letter or message to that office and the following information addressees: HQ AFCA/GCOM, the parent MAJCOM/DRU/FOA, and HQ SSG/DIGC.

3.10.1.2. NCCs will notify the affected ROSC via telephone. Follow up with a letter or message to the ROSC for action and information copies to the parent MAJCOM, DRU, or FOA.

3.10.2. Routine Deficiency Reports (Categories 2, 3, and X).

3.10.2.1. TCCs will send a message or letter to the originator's immediate higher headquarters. Send information copies to HQ AFCA/GCOM and HQ SSG/DIGC. If the MAJCOM, FOA, or DRU is not the immediate higher headquarters, send an information copy to the parent MAJCOM, DRU, or FOA.

3.10.2.2. NCCs will send a message or letter to the affected ROSC. Send information copies to the parent MAJCOM, FOA, or DRU and HQ SSG/SIDI.

3.11. Customer Support. Develop local procedures for quarterly customer visits and user group meetings, and develop customer education programs or questionnaires to make sure customer requirements are met and the mission requirement is fully supported.

Section D—Software Processing

4. Software Releases. The MC or DPC manager, or a designated representative will enter software changes into an operating unit's operational software when the applicable software support office releases the software change. Units will notify the software support office when the software upgrade is implemented.

5. Organizational Responsibilities for Deficiency Processing.

5.1. MAJCOMs and DMS ROSCs will review and evaluate deficiency reports and send a message to the appropriate software support office to resolve. Include HQ SSG/SIDI and HQ SSG/DIGC as information addressees on all DMS correspondence.

5.2. The software support office designs, codes, certifies, and releases software changes to the field in response to emergency deficiencies.

5.3. Units implement software changes on receipt. Within 24 hours of patch implementation, units will notify the applicable software support office of patch implementation by sending an operational software implementation notice as shown in **Attachment 4**. Units close a deficiency if they cannot recreate it or if it does not recur within 30 calendar days.

Section E—Message Handling and Administrative Procedures

6. Policy, Procedures, and Guidance. ACP 121 USSUP1(); JANAP-128(), *Automatic Digital Network (AUTODIN) Operating Procedures*; Air Force Instruction (AFI) 33-115, *Networks Management*; AFI 33-119, *Electronic Mail (E-Mail) Management and Use*; AFI 33-129, *Transmission of Information Via the Internet*; and various DISA publications contain specific policies, procedures, and guidance for the operation and management of AUTODIN TCCs and Air Force NCCs (AFNCC).

6.1. Authorized Users of the AUTODIN System. Limit use of AUTODIN to official business that cannot be sent by other forms of electrical transmission. See AFI 33-119 for using commercial e-mail and AFMAN 37-126, **Attachment 2** (to become AFMAN 33-326), for authorized AUTODIN users.

6.2. Minimize. MINIMIZE is a messaging requirement service for AUTODIN and DMS that applies to both organizational and individual users. Users of AUTODIN and DMS must adhere to MINIMIZE when imposed.

6.2.1. The objective of MINIMIZE is to clear communications and information systems of traffic whose urgency does not require transmission by electrical means during an actual or anticipated emergency. Commanders at all levels have the authority to impose MINIMIZE within their command or area of command responsibility unless specified or denied by appropriate higher authority.

6.2.2. During MINIMIZE, electrical transmission is justified only to avoid serious detrimental impact on mission accomplishment or to save lives.

6.2.3. MINIMIZE is imposed on message originators and releasing authorities. When MINIMIZE is imposed, commands will:

6.2.3.1. Establish rigid procedures to ensure that messages not meeting the MINIMIZE criteria are forwarded by other means (e.g., mail, courier, etc.). Do not hold record communications for transmission pending cancellation of MINIMIZE. This practice could seriously overload the network after the MINIMIZE is canceled.

6.2.3.2. Originators and releasing authorities must review all messages to ensure that those not meeting MINIMIZE requirements are sent by other than electrical means and those messages that are electrically transmitted are concise and addressed to the minimum number of addressees.

6.2.3.3. Require releasing authorities to state "MINIMIZE CONSIDERED" on the message release document. Do not place "MINIMIZE CONSIDERED" in the message text.

6.2.4. When MINIMIZE is canceled, commanders will ensure a review is made of the messages transmitted during MINIMIZE to check the effectiveness of MINIMIZE policies and procedures and take action to correct deficiencies. See ACP 121, USSUP1 and ACP 123, USSUP1 for further information.

7. Telecommunications Center Message Handling Procedures.

7.1. Incoming Message Processing. TCC personnel will:

7.1.1. Process all incoming messages in order of precedence on a first-in-first-out basis.

7.1.2. 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.

7.1.3. 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.

7.1.4. Notify the "action" addressees on receipt of IMMEDIATE and higher precedence messages. If a message management letter is not on file at the TCC, call the organization commander, deputy commander, or the appropriate directorate chief. **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.

7.1.5. Read messages over the telephone when it is imperative to notify an individual about a casualty situation such as a Red Cross message, or when unclassified high precedence messages are routed to an alternate delivery station and distance precludes timely delivery.

7.1.6. Notify the addressee on receipt of an emergency command precedence (ECP) message (e.g., emergency action message [EAM], FLASH, RED, and WHITE ROCKET messages).

7.1.7. Distribute one copy of each message to the appropriate 2-letter internal distribution office or single office for an organization. Exceptions to the 2-letter internal distribution can be made to accommodate electronic delivery of AUTODIN message traffic. **NOTE:** Because of the nature and urgency of message traffic that a COMSEC account receives, direct message release to the COMSEC account is authorized. Address COMSEC account messages to the local communications unit using CA and its designated six numeric characters.

7.1.8. Use BITS or the base network (e-mail) 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 unsecure networks.

7.1.9. 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 [NOFORN] or Atomic Energy Restricted) and all classified messages requiring receipt in compliance with Department of Defense Regulation (DoDR) 5200.1, *DoD Information Security Program*, January 1997; AFPD 31-4, *Information Security*; and AFI 31-401, *Managing the Information Security Program*, directly to the addressee or designated representatives of the addressee.

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

7.1.11. Place unclassified messages in a plain envelope or Optional Form (OF) 65C, **U. S. Government Messenger Envelope**, to send through BITS.

7.1.12. Deliver TOP SECRET messages according to DoDR 5200.1, AFPD 31-4, and AFI 31-401. Deliver TOP SECRET Special Category (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. The TCC must place all SPECAT, TOP SECRET, Inspector Distribution (INSPECDIS), and other privacy messages in an AF Form 3530 before delivering them.

7.1.13. Deliver PERSONAL FOR messages to the individual named or a designated representative. The following rules apply to PERSONAL FOR messages:

7.1.13.1. Customers may have their PERSONAL FOR messages delivered to a personal e-mail box (reference AFI 33-119).

7.1.13.2. Do not re-address.

7.1.13.3. Place in an AF Form 3530 and hold for pickup.

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

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

7.1.13.6. The use of the caveat "PERSONAL FOR" will be authorized for use only by general/flag officers and civilians of equivalent rank (reference ACP 121(), paragraph 320b).

7.1.14. Place drug testing messages received with the phrase "DBMS EYES ONLY" (where DBMS means Director Base Medical Services) at the end of the classification line in an AF Form 3530 before delivery.

7.1.15. Place Critical Nuclear Weapon Design Information (CNWDI), Cryptographic, Restricted Data, 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 DoDR 5200.1, AFPD 31-4, and AFI 31-401.

7.1.16. Use the 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.

7.1.17. Receive Electronic Warfare Integrated Reprogramming (EWIR) messages on a diskette that does not contain any other messages. Do not attempt to change or correct EWIR messages. **NOTE:** EWIR messages are both real world (PACER WARE) and test (SERENE BYTE).

7.1.18. General Messages. General messages addressed to customers (such as All Food Activities [ALFOODACT], etc.) do not require logging or retention past that of other regular message traffic. Log general messages addressed to the TCC (e.g., Joint Armed Forces Publications, All Military Activities [ALMILACT], Network Control Message, etc.) on AF Form 3532, **General Message Record**, and file sequentially. The first general message of each year provides disposition and destruction authority for the previous year's general messages. Track general messages chronologically for the current year.

7.1.19. File the local office symbol address with the customer-provided list of AIG local addresses.

7.1.20. Keep a current list of individuals authorized to pick-up and receive messages. The source document for identifying authorized users is the message management letter (MML). Users should update MMLs quarterly.

7.2. Outgoing Message Processing. TCC personnel will:

7.2.1. Protect information against loss or compromise.

7.2.2. Process messages first-in-first-out by precedence. Process high precedence messages expediently and provide status to supervisory personnel.

7.2.3. Assign station serial numbers manually if equipment does not automatically assign them. 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.

7.2.4. Assign routing indicators, if applicable.

7.2.5. Proofread the entire message if prepared manually.

7.2.6. Where applicable, 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.

7.2.7. Write the time of transmission if equipment does not have an automatic journal or log.

7.2.8. File messages sequentially by station serial number, time of file, or date-time-group per local procedures.

7.2.9. 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.

7.2.10. The releaser's organization reproduces additional copies of outgoing messages before delivery to the TCC. Delivery to ZEN 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. Do not provide originators with comeback or file copies. TCCs may self-address operational readiness inspection (ORI) exercise messages into AUTODIN to evaluate ability to manually process traffic by using the following criteria:

7.2.10.1. Give the affected ASC 8 hours prior notification, by message, of the introduction of self-addressed test message traffic.

7.2.10.2. The notification message will consist of date and time of test start, approximate number of messages to send, name and telephone number of ORI point of contact (POC), and name of TCC getting evaluated.

7.2.10.3. Assign a block of station serial numbers to remote terminals to identify specific remotes according to local instructions.

7.2.10.4. Submit high volume message inputs according to DISAC 310-70-30.

7.2.11. 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 DoDR 5200.1, AFPD 31-4, and AFI 31-401.

7.2.11.1. Establish handling procedures which:

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

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

7.2.12. 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 USSUP1() for further guidance. Types of SPECAT messages:

7.2.12.1. ECP Messages (EAM, FLASH, RED, and WHITE ROCKET].

7.2.12.2. EXCLUSIVE FOR. Example: SECRET SPECAT EXCLUSIVE FOR GEN SMITH. **NOTE:** Do not use terms or phrases such as "EYES ONLY”, "PERSONAL FOR", etc., on SPECAT messages.

7.2.12.3. 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.

7.2.12.4. Other Special Handling Message Types:

7.2.12.4.1. TOP SECRET.

7.2.12.4.2. PERSONAL FOR. General/flag officers and civilians of equivalent rank originate PERSONAL FOR messages. The caveat "PERSONAL FOR" means you must protect the privacy of the message.

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

7.2.12.4.4. CNWDI.

7.2.12.4.5. INSPECDIS.

7.2.12.4.6. Drug Testing.

7.2.13. Scan all diskettes for viruses.

7.3. Use of LANs for Record Message Distribution.

7.3.1. Electronic sorting and distribution of message traffic within an organization will not be restricted to functional address symbols.

7.3.1.1. Profiles to distribute record messages on a LAN will be established to identify and limit distribution of sensitive subject messages, through use of key word searches, to authorized personnel only.

7.3.1.2. Distribute other organization message traffic, not restricted due to subject or program, through the use of key word searches, without restriction to functional office symbols.

7.3.2. Distribute messages with special handling designators, special delivery instructions, or other caveats restricting distribution across a LAN provided the operating software of the systems where messages reside and the software controlling viewing of the messages is able to limit access to authorized personnel and prevent anyone else from unauthorized or inadvertent access.

7.4. Correcting Message Preparation Errors.

7.4.1. Major errors preclude transmission of the message (i.e., incomplete or incorrect address element which the TCC cannot correct, security mismatch, no releaser's signature, improperly prepared or unreadable diskettes, TOC/CRC mismatch, etc.). In these cases, the TCC operator follows local procedures for contacting releasing officials or fills out a Department of Defense (DD) Form 1503, **Message Correction Notice**, and promptly returns ROUTINE messages with the form to the releasing officials for reaccomplishment or correction. For PRIORITY or higher precedence messages, the operator immediately notifies the releasing official or agency to initiate corrections. If unable to reach the releasing official follow local procedures for notification.

7.4.2. Minor errors do not preclude further processing of the message. The operator coordinates with the releasing official or message drafter, if necessary, to resolve specific preparation errors. The operator then processes and transmits the message and follows local procedures for notifying the originator.

7.5. Service Messages. Use service messages for exchanging information to speed up, correct, clarify, report, or ease the flow of message traffic. Also use them to deal with anticipated workloads of an unusual nature, SPECAT information or information requiring special handling, the adjustment of procedural discrepancies, or changes to available facilities. All service messages must conform to rules of transmission and COMSEC. Use only authorized and appropriate operating signals and prosigns for service messages. Refer to ACP 127 USSUP1(), *Communications Instructions Tape Relay Procedures;* ACP 131 USSUP1(), *Communications Instructions Operating Signals;* and JANAP 128() for further guidance.

Section F—Message Terminal Operations

8. Introduction. The message terminal (MT) does various processing jobs including automatic message formatting and routing, automatically determining incoming distribution, and switching messages to and from AUTODIN, other MTs, and its own tributary stations.

8.1. Remote terminals and tributary stations are personal computer (PC)-based platforms and vary in configuration.

8.2. Customer-operated tributary stations usually support a dedicated mission and possibly one or two other customers. Their work includes only those systems functions necessary to send and receive the tributary station's information. They rely on the MT as a network control station.

8.3. Other tributary stations may support a single dedicated user, multiple users, or may act as a TCC.

8.4. Personnel operating messaging terminals at tributary stations must:

8.4.1. Protect information against loss or compromise.

8.4.2. Follow security practices.

8.4.3. Follow COMSEC procedures.

8.4.4. Help the TCC in obtaining a unique routing indicator.

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

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

8.5. The MT acts as the control station for its remote tributary stations. MT personnel will:

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

8.5.2. Give technical assistance and training.

8.5.3. Maintain system control to minimize operational impact of failures to tributaries, the MT, or the connected ASC.

8.5.4. 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.

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

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

Section G—Storage Media Management

9. Storage Media Libraries.

9.1. Storage Media Procedures. The MC or DPC manager must set up procedures that cover control, security, and upkeep of all storage media.

9.1.1. External tape or disk identification. Use magnetic media labels and guidelines as prescribed in DISAC 310-70-30 and DoDR 5200.1, Chapter 5. Ensure effective management and control by putting the following items on the outside of the tape reel, floppy disk, disk pack, or cartridge (**NOTE:** Place information marked with an asterisk [*] on the outside of the magnetic medium [e.g., tape reel, disk pack cartridge, or floppy disk]. The TCC manager stores all other information elsewhere):

9.1.1.1. *Organizational identification.

9.1.1.2. *Reel or disk pack/cartridge number (tape reel or disk pack cartridge only).

9.1.1.3. *Recording density.

9.1.1.4. *Security classification.

9.1.1.5. *Acquisition date (tape reel or disk pack cartridge only).

9.1.1.6. *Operating system (floppy disk only).

9.1.1.7. Physical characteristics (length, width, hub size, number of disks, compatible drive, etc.).

9.1.1.8. Usage record (including cleaning).

9.1.1.9. Error reports.

9.1.1.10. Final disposition.

9.1.1.11. Physical location.

9.1.2. Internal Tape Identification. The internal identification of tapes is software-controlled information. Include the title, file number, reel of file, date written, purge date (date the data becomes obsolete and the tape may be reused), classification, and declassification instructions in this information.

9.2. Cleaning or Rehabilitation Cycle. Keep a record, by reel, pack, or cartridge number, of the date serviced. Turn in items no longer usable to the local Defense Property Disposal Agency (DoD Manual [DoDM] 4160-21, *Defense Reutilization and Marketing Manual*, March 1990). Degauss all items with classified or personal information and remove any labels or documentation attached that could reveal the previous contents of the degaussed tape or its sensitivity before turning them in. AFSSI 5020, Remanence Security, provides guidance.

9.3. Inventory Accountability. Library records 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. Control and inventory of classified magnetic media in the library is prescribed in DoDR 5200.1 and AFI 31-401.

9.4. Care, Handling, and Maintenance of Magnetic Media. Personnel who work with magnetic media must maintain and use them according to local instructions.

9.4.1. Shipping Magnetic Tapes:

9.4.1.1. Make sure the outer container is water resistant and strong enough to protect the tape from damage.

9.4.1.2. Mark the outer container with "FRAGILE, MAGNETIC TAPE, KEEP AWAY FROM ELECTRIC MOTORS, SCANNING DEVICES, AND MAGNETICS”, or use an OF 85, **Fragile-Magnetic Tape Label**.

9.4.1.3. Mark, ship, and safeguard classified magnetic media according to DoDR 5200.1 and AFI 31-401.

9.4.2. Immediate Access Storage (IAS) Management:

9.4.2.1. Set up disk management standards governing programs and files allowed to reside on disks.

9.4.2.2. Keep only necessary programs and files on disks.

9.4.2.3. Backup critical programs, disk resident files, system software routines, production programs, and data files on tape and store in a secure location away from the facility.

9.4.2.4. Furnish guidelines and set up controls within MC and DPC operations for the following areas:

9.4.2.4.1. Loading and removing programs and files.

9.4.2.4.2. Verifying the validity of program versions and backups.

9.4.2.4.3. Overseeing the status of checker boarding and schedule compacting procedures.

9.4.2.4.4. Running disk analysis programs to check disk use.

9.4.2.4.5. Applying procedures for care and control of IAS hardware.

9.4.3. Storing Magnetic Media:

9.4.3.1. On-site storage. Store computer programs and data files in a fire-retardant vault area or in fire-retardant cabinets (when feasible).

9.4.3.2. Off-site storage. Keep selected files, to include operations programs, system builds, database directories, etc., in a secure area physically separated from the MC or DPC. Select the off-site storage location based on its proximity to the MC or DPC, the temperature and humidity, and the physical security of the building. Place a priority schedule for recreating files, as well as those products specified in other areas of this publication, at the off-site storage location.

Section H—Defense Message System

10. Introduction. The Air Force has a mission-critical need for flexible, deployable, and joint messaging communication service in both peace and contingency situations. To meet the mission critical need of timely and accurate messaging at all levels of command, the DMS will migrate narrative organizational messaging traffic from the aging AUTODIN system to a secure writer-to-reader messaging system. The flexibility of this system to support the in-garrison and deployed wings will enhance the Air Force communications unit’s ability to provide real-time messaging services regardless of the location or desired service.

10.1. Architecture and Staffing. The NCC will control and centrally manage DMS resources on Air Force bases or sites regardless of the implemented architecture. See AFI 33-115 for NCC management policies.

10.1.1. The NCC will perform DMS functions and will use existing AUTODIN TCC manpower. Therefore, align the TCC functionally with the NCC to facilitate efficient personnel management.

10.1.2. Ideally, you will physically locate the NCC and TCC together to reduce space and manpower requirements. However, where that is not possible due to facility restrictions, NCCs should develop strategies to eventually physically consolidate the TCC and NCC upon elimination of the legacy AUTODIN TCCs.

10.1.3. Align the certification authority workstation (CAW) users certification authority, SA, and CSSO within the wing IP office. The wing COMSEC manager is responsible for the CAW functions and will also have overall management of the registration function that is performed by the organization registration authorities (ORA).

10.1.4. For DMS users, the NCC Help Desk (HD) is the primary POC for reporting system problems, reporting transport network problems, and requesting technical assistance. Supervisors will ensure HD personnel are familiar with the operations, management, security services, and directory services of the DMS.

10.1.5. The wing IP office performs all CA and registration activities, including the CAW function which is located within the COMSEC account. The CA will use the CAW to perform their day-to-day duties such as key/certificate generation and FORTEZZA card programming.

10.2. Directory Registration. The comprehensive, automated DoD-wide directory in DMS will simplify the search for information, provide more accurate addressing, and eliminate the need for the releasing authority to validate the originator's address. The DMS directory is the single authoritative source of directory information for both organizational and individual messaging users. A user/organization is considered registered when an entry is input in the directory or a FORTEZZA card is created and issued. Registration requirements, sub-RA and ORA responsibilities, and directory maintenance procedures are identified in AFI 33-127, *Electronic Messaging Registration and Authority*, and AFMAN 33-128, *Electronic Messaging Registration*.

10.3. Directory Shadowing. A process called "shadowing" allows you to duplicate directory information from a DSA in another global or local DSA. Determination of information that will be shadowed is laid out in shadowing agreements between managers of the DSAs involved. Each local DSA contains a portion of the Directory Information Base (DIB) for which it is designated "master". Update shadow DIBs from the master within ten minutes of a change in the master.

10.3.1. Global Level Replication. DISA maintains and designates one DSA as the master DSA. Other global DSAs will establish a shadowing agreement with the DISA-designated master DSA and replicate this information. Each activity maintaining a global-level DSA is responsible for establishing a shadowing agreement with at least one other global-level DSA.

10.3.2. Local Level Replication. Each local-level DSA subordinate to a global-level DSA is responsible for establishing a shadowing agreement with a global-level DSA in order to receive a replicated copy of the global directory information tree (DIT) structure. Each activity maintaining a local-level DSA is also responsible for establishing a shadowing agreement with at least one other local-level DSA. Establish these shadowing agreements in such a manner as to prevent a single point of failure.

10.3.3. Directory Shadowing Procedures. Ensure directory shadowing procedures are included in Annex K to the operations plans (OPlan).

10.4. Directory Browsing. Directory browsing, the search of the directory for message recipient information, is permitted by the directory system. However, since browsing consumes network resources, you should only do it when necessary for message transmission or other official use. Do not allow browsing out of curiosity or for purposes unrelated to official duties.

Section I—Defense Message System Message Handling and Administrative Procedures

11. Defense Message System Message Handling and Administrative Procedures.

11.1. DMS System Backups. While most DMS components are designed to operate continuously in an unattended mode, some administrative functions are periodically required. The principal one of these is the system backup. A backup in this case means the transfer of log and audit data from the system internal storage (hard disk) to an external storage device (diskette or tape) for the required retention period. Backup requirements are:

11.1.1. Keep daily incremental backups for 1 weekly backup cycle. Save them daily every 24 hours at the change of the radio day (RAYDAY).

11.1.2. Retain weekly full backups for two cycles.

11.1.3. Rotate most recent copy of the weekly full backups to an off-site location.

11.1.4. Send the original copies of all DMS software and operating system programs to the off-site location.

11.2. Message Delivery/Traceability. Message tracing is the process whereby an originator can request a message previously submitted to the DMS be traced through the system to its final disposition. Message tracing is initiated by an originator reporting a trouble report to the NCC HD. Confirmation of message delivery is an originator/receiver responsibility. The NCC HD will:

11.2.1. Provide customer education on message trace procedures.

11.2.2. Limit message trace requests to within 30 days after the original message was sent. Requests must contain the user's message identification information, the recipients of the message, and the time of submission.

11.2.3. Initiate a trouble ticket documenting the trace request.

11.2.4. Notify the originator of the final results of the trace action.

11.2.5. Provide a full response to trace requests within 72 hours of the request.

11.2.6. Raise the trace trouble ticket to the ROSC if you must continue the trace outside the NCC AOR.

11.2.7. Use service messages to exchange information to speed up, correct, clarify, report, or ease the flow of message traffic. Also use them to deal with anticipated workloads of an unusual nature, the adjustment of procedural discrepancies, or changes to available facilities.

11.3. Message Retention. All messages originated, stored, or received in DMS are federal records. It is the user's responsibility to maintain record copies of messages in accordance with AFMAN 37-139, *Disposition of Records-Records Disposition Schedule* (to become AFMAN 33-339). In addition, users must:

11.3.1. Ensure accessibility of on-line audit trails and logs within 10 minutes, and off-line records within 4 hours.

11.3.2. Store all incoming and outgoing messages at the user component for a minimum of 10 days, providing on-line retrieval of less than 10 minutes.

11.4. Alternate Routing/Delivery Points.

11.4.1. Organizational user accounts must stay manned on a 24-hour, 7-day basis (24/7), or arrange for an alternate delivery point for high-priority traffic when not manned.

11.4.2. Staff alternate delivery points and keep them operational during the time it will serve as an alternate. Staffing of alternate delivery points must be determined between sites.

11.4.3. An alternate delivery user must share a private key with the normal recipient.

11.4.4. For DMS clients who are not manned 24/7, implement auto-forward capability to ensure delivery of URGENT messages to a 24/7 POC. Once auto-forwarded, responsibility for notification of URGENT traffic rests with the 24/7 POC. If a message management letter is not on file at the POC, the 24/7 POC will notify the organization commander, deputy commander, or the appropriate directorate chief.

11.4.5. The MC reads messages over the telephone to verified recipients when it is imperative to notify an individual about a casualty situation such as a Red Cross message, or when unclassified high precedence messages are routed to an alternate delivery station and distance precludes timely delivery.

11.5. Releasing Authority.

11.5.1. The releasing authority must continue to perform the same validations to authorize the release of an outgoing message as in the AUTODIN process. However, rather than forwarding the message to the TCC for transmission, the releasing authority will transmit the message directly over the Defense Information Systems Network (DISN) via a DMS user agent.

11.5.2. Commanders restrict authority to release FLASH messages to general and flag officers, civilian equivalents, and commanders, or their representatives specifically authorized in writing.

11.5.3. Commanders must tightly restrict delegation of authority to release IMMEDIATE, ECP, and FLASH messages. ECP, FLASH, and IMMEDIATE messages will have as few information addressees as possible. Make the precedence for information addressees ROUTINE.

11.6. Fault Management. Fault management is the detection, isolation, and correction of failures or problems in, or abnormal operation of, DMS components. The ability to detect and correct service-affecting problems ensures that DMS services are provided at the required level. Fault detection is a function of a DMS management process that consists of software within each DMS component reporting faults to the appropriate management workstation (MWS).

11.6.1. Fault Reporting and Analysis. NCC personnel receiving an indication of a component fault must log the report and attempt to determine the cause. When it appears that the problem is localized in a particular component, and remote restart capability exists, attempt a restart. If the restart is not successful, contact the SA responsible for that component and submit a trouble ticket. When the on-call technician is at distance from the site, and where there is no obvious hardware failure, the SA should attempt to resolve the problem. When a hardware failure is obvious, or when the problem cannot be resolved within one hour, contact the technician, either by the writing of a trouble ticket or by other means (such as the telephone).

11.6.2. Fault Management Functional Duties. Functional duties of fault management include:

11.6.2.1. Installing monitoring tools and support software.

11.6.2.2. Defining alerts or traps.

11.6.2.3. Configuring management system reporting processes to transmit to specific MWSs.

11.6.2.4. Diagnosing causes of alerts and taking corrective action to resolve and prevent them.

11.6.2.5. Planning and implementing fault tolerance mechanisms.

11.6.2.6. Restoring component operation or implementing routing changes to bypass failed components.

11.6.2.7. Performing recovery for components that store message traffic.

11.6.2.8. Supporting the HD for problem detection, isolation, resolution, and prevention.

11.6.2.9. Analyzing audit logs and performance data as necessary to anticipate and preempt faults.

11.7. Configuration Management. Configuration management (CM) is the application of technical and administrative direction and surveillance to identify and document the functional and physical characteristics of a configuration item and to control and record changes to those items. The configuration item may be a single component or a whole system. Several functions that make up CM include:

11.7.1. Managing the inventory and locations of deployed components.

11.7.2. Managing system and component functionality, including a review process for system changes.

11.7.3. Provisioning user service, including activation, change, and deactivation of users.

11.7.4. Configuring, activating, modifying, and deactivating system components.

11.7.5. Implementing DSA shadowing procedures.

11.7.6. Establishing authentication processes for DMS components.

11.7.7. Reconfiguring DMS components for performance improvements or problem resolution.

11.7.8. Procuring, changing, or releasing internet protocol addresses for DMS components.

11.7.9. Maintaining a system configuration data base.

11.7.10. Controlling component hardware platforms.

11.7.11. Controlling component software.

11.7.12. Controlling component inventory and providing spares as needed.

11.7.13. Acquiring and applying system software changes (patches) between releases.

11.8. Performance Management. Performance management is based on performance monitoring that provides management with tools to judge the reliability, availability, and speed of service of the DMS.

Some performance monitoring is based on information available on a real-time basis and is used by network managers to evaluate network performance and correct trouble conditions as they occur. The NCC must pay particular attention to the established standards and thresholds, because if they are exceeded management action might be required. The standards and thresholds that could cause local or regional management action include:

11.8.1. Backlog conditions.

11.8.2. Excessive processing time.

11.8.3. Delay of high precedence messages.

11.8.4. Denial of service.

11.8.5. Delays within a DMS component.

11.9. Data Collection. The data collection area of network management involves the gathering of statistical information on which to base future changes to the network. Data may be collected in real time (at the time of the event to be recorded) or in historical time (sometime after the event). In practice, data collection is usually a combination of the two, with a DMS component logging events as they occur, and a management component or workstation retrieving the log data at some convenient time (such as the end of the day) and processing it for further analysis. This type of analysis can produce statistical information that is used by management to find network bottlenecks, determine the need for network expansion, or adjust network configuration.

Section J—Defense Message System Mail List Management

12. Mail Lists. MLs provide the ability to use a single abbreviated name to send messages to a predetermined list of not less than 16 organizational addresses, called the composition of the ML.

12.1. Use MLs only for organizational messaging. MLs distinguished names (DN) are entries under a tree in the DMS International Telecommunication Union-Telecommunications (ITU-T) recommendation X.500 (Information Technology - Open systems interconnection - The Directory) DIT.

12.2. There are two types of MLs: numbered and collective titles/joint general message titles.

12.3. The Military Communications-Electronics Board (MCEB) allocates ML numbers in blocks to the Air Force ML control authority.

12.4. Each ML has its own DMS originator/recipient (O/R) address. The address is that of the mail list agent (MLA) on which the ML resides.

12.5. Each ML also has a certificate and a key registered in the directory.

12.6. The DSA that provides direct support to the MLA, that processes messages for the ML, maintains the ML directory.

12.7. An ML is considered classified when at least one address in the composition has been assigned a classification of CONFIDENTIAL or higher. In the event a ML is unclassified and it is necessary to send a classified message to the ML, mark the text of the message according to DoDR 5200.1, but the ML itself is not classified.

12.8. Each ML has a control authority, a cognizant authority, a manager, members, and users.

13. Control Authority. HQ AFCIC/SYNT is the Air Force control authority for MLs.

13.1. The Air Force control authority will make block assignments of MLs to the MAJCOM, DRU, and FOA ML managers.

13.2. When the control authority changes an AIG to an ML, the control authority assigns the same number to the ML as was assigned to the AIG. For example, AIG 123 will become ML 123. The control authority will cancel those AIGs not converted to MLs at the time AUTODIN is closed and will retain those numbers for future assignment.

14. Cognizant Authority. Each ML must have a cognizant authority. The cognizant authority determines the need for a ML, controls its use, and is the ML owner and primary user. The cognizant authority will:

14.1. Request assignment of a ML from the control authority.

14.2. Review the directory before applying for a numbered ML assignment to determine whether one is already registered with the same purpose. If another ML does not already exist, so state in the application for a ML. If a ML does exist with the same purpose:

14.2.1. Contact the POC for that ML to find out the composition. If the composition is the same as that used for the new ML, the two organizational POCs should coordinate shared usage. If the POC for an existing ML does not agree to share usage, the control authority will intervene and determine if shared usage is appropriate.

14.2.2. If a mission-essential requirement exists to duplicate the composition and purpose of an existing ML, provide justification that clearly explains the mission need for the duplication to the ML control authority. The ML control authority will approve or disapprove the request.

14.2.3. Notify the ML control authority whether the AIG will be retained for use during transition or that the POC will take action to cancel the AIG immediately upon establishment of the ML in the directory.

14.2.4. Coordinate the registration of an assigned ML with the ML manager.

14.2.5. Identify the composition and authorized users of the ML to the ML manager.

14.2.6. Keep abreast of any changes in ML member status, such as change of address or organizational name, and advise the control authority and the ML manager of changes.

14.2.7. Send the first message to the ML after registration is completed to promulgate its existence, purpose, the authorized users, the composition, and whether it is classified.

14.2.8. Delete obsolete MLs and notify the control authority, the ML manager, and ML members of the deletion.

14.2.9. Review and validate MLs using the same procedures already in place for AIGs.

15. Mail List Manager. The ML manager represents the cognizant authority of a ML for creating, changing, and deleting the ML. The ML manager will:

15.1. Create, change, and delete the ML in the directory using an administrative directory user agent (ADUA) within 3 days after notification from the cognizant authority that one of these actions is required.

15.2. Obtain and install a FORTEZZA card for the MLA.

15.3. Ensure that the composition and authorized users of a ML are kept current.

15.4. Maintain references ("backpointers") from the ML member entry to the ML entry.

15.5. Notify the ML cognizant authority when required changes to the directory or the ML have been effected or of any reason changes cannot be accomplished.

15.6. Notify the cognizant authority of a new ML manager and MLA when a ML is moved to another MLA.

15.7. Coordinate with the NCC or ROSC in resolving ML operational problems.

15.8. Receive, check, and approve or disapprove requests for ML assignments.

15.9. Issue ML numbers to requesting authorities.

15.10. Keep a current list of ML assignments with related ML information.

15.11. Coordinate with the regional service manager (RSM) to determine which MLA will serve each ML.

16. Mail List Members. ML members are those organizations identified by the cognizant authority that make up the composition of the ML. ML members will:

16.1. Stay knowledgeable of all the MLs for which they are part of the composition.

16.2. Notify the ML cognizant authority to remove themselves from an ML.

16.3. Contact the ML cognizant authority to add themselves to the composition of a ML. Addition requests should contain mission-essential justification.

17. Mail List Users. ML users are those organizations authorized to send messages to the ML.

17.1. The cognizant authority of a ML is normally the only authorized user. The cognizant authority will identify other users to the ML manager as necessary.

17.2. ML users are typically members of the composition of the ML, but not necessarily.

17.3. Organizations that are not currently identified as users of a ML must coordinate with the cognizant authority to become a user.

17.4. ML users are responsible for:

17.4.1. Knowing whether the ML is classified.

17.4.2. Knowing the composition and purpose of the ML.

17.4.3. Knowing of any special handling requirements for messages addressed to the ML.

17.4.4. Notifying the cognizant authority of the ML whenever their address changes or to remove themselves as a member of the composition.

17.4.5. Notifying the cognizant authority and ML manager of any problems encountered.

18. Mail List Composition. The composition of a U.S. ML, whether it is a number or a collective title/joint general message title, will only contain U.S. addresses. Avoid the duplication of numbered MLs to the maximum extent possible.

18.1. You may add non-U.S. addresses on messages sent with a U.S. ML. For example, the address of ML 123 and the non-U.S. address of Ministry of Defense United Kingdom (MODUK) could each appear as the two message addresses. The MCEB will consider exceptions on a case-by-case basis.

18.1.1. The control authority will process requests received from cognizant authorities for exceptions to policy to mix U.S. and non-U.S. addresses in the composition.

18.1.2. When the control authority deems the request valid, they will sponsor a formal request for approval of the exception to the MCEB. The MCEB has final approval authority for all exceptions and maintains a master list of those that have been granted.

18.2. The ML control authority will prevent duplication of composition and purpose of numbered ML to the maximum extent possible. Requests for exception process:

18.2.1. The control authority will review requests for numbered ML duplication. They may grant approval for those requests that contain clearly defined mission-essential justification.

18.2.2. In the event the control authority cannot approve a request for duplication of a numbered ML, they will intervene with the cognizant authority of the duplicated ML to negotiate sharing.

18.2.3. The control authority may direct the cognizant authority of a numbered ML to share usage to prevent duplication to the maximum extent.

18.3. A ML is considered classified when at least one of the addresses in the ML composition is classified. When the text of a message sent to a ML is classified it does not make the ML classified.

19. Collective Title/Joint General Message Title. Never duplicate the composition and purpose of a collective title/joint general message title.

19.1. The control authority will review requests to establish MLs that use collective titles/joint general message titles and maintain a master list of those assigned. The ML control authority will forward those requests that meet the specified requirements to DISA for processing.

19.2. Rationale for establishing a ML with a collective title/joint general message title must contain mission-essential justification that explains why assignment of a number for the ML common name will not meet mission needs.

19.3. Collective titles/joint general message titles will consist of no more than two words or acronyms and cannot exceed 20 characters in length. Most of the collective titles/joint general message titles assigned for use on AUTODIN will convert to MLs.

19.4. The control authority will establish a method to assign sequential numbers by year to each collective title/joint general message title message. Duplication of numbers within a given year is prohibited. The control authority will ensure the first message of each calendar year (i.e., 1/98) sent to a collective title/joint general message title contains a list, by year, of all the active messages. When 1/(year) is received, recipients must retain those listed in the text of the first message and may destroy those messages not listed. For example, ALMILACT 1/98 may state that you must retain 2/96, 10/96, and 50/97, which means you should destroy ALMILACT messages prior to l/96, as well as those not listed for the years of 1996 and 1997.

20. Mail List Agent. The MLA is a DMS infrastructure component that simplifies the distribution of a message to multiple recipients. The DMS compliant O/R address for the MLA is registered in the directory and is the O/R address for each ML resident on that MLA.

20.1. The MLA receives messages addressed to MLs for which it is responsible. It expands the ML name to the composition (list of recipient organizations), creates a new message with the original text for each of them using the DMS compliant organizational O/R address, and sends them each the message.

20.2. Many MLAs will exist in the DMS network, each of which will contain a data base with the composition of each ML for which it is responsible. When an authorized user of a ML accesses the directory through their UA for the ML address, the address received is that of the MLA serving the ML.

Section K—Defense Message System Security

21. Defense Message System Employs Writer-to-Reader Security. Messages that require security protection are encrypted from originator to recipient, or end-to-end. Messages are encrypted before leaving an originator's equipment and are not decrypted until reaching an authorized recipient, the actual intended recipient, an authorized alternate, or a DMS component.

21.1. DMS uses digital signatures to validate authenticity of received messages and messages released for the organization. Digital signatures allow authentication of involved persons, prevent undetected alteration, and provide an electronic record of the message.

21.2. DMS will encrypt all messages with some very limited exceptions. In such cases, releasers must sign messages to provide originator authentication and non-repudiation.

22. Management Checklist. To help you better manage the tasks imposed by this publication, you may use the questions at **Attachment 5** and AF Form 2519.

23. Addresses:

23.1. HQ AFCIC/SYNT, 1250 Air Force Pentagon, Room 5B520, Washington DC 20330-1250.

23.2. HQ AFCA/GCOM, 203 West Losey Street, Room 3065, Scott AFB IL 62225-5233.

23.3. HQ SSG/SIDI/DIGC, 501 East Moore Drive, Maxwell AFB-Gunter Annex AL 36114-3312.

24. Forms Prescribed. This instruction prescribes 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**; DD Form 1503, **Message Correction Notice**; and OF 85, **Fragile-Magnetic Tape Label**.

WILLIAM J. DONAHUE, Lt General, USAF
Director, Communications and Information

Attachment 1

GLOSSARY OF TERMS AND SUPPORTING INFORMATION

References

ACP 121 USSUP1, (C) *Communications Instructions-General (U)*

ACP 123 USSUP1, *Common Messaging Strategy and Procedures*

ACP 127 USSUP1, *Communications Instructions Tape Relay Procedures*

ACP 131 USSUP1, *Communications Instructions Operating Signals*

AFSSI 5020, *Remanence Security*

AFSSI 6001, *Operational Instruction for Components and Systems Supporting the Multilevel Information Systems Security Initiative (MISSI)*

DISAC 310-70-30, *DCS AUTODIN Switching Center and Subscriber Operations*

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

DoDM 4160.21, *Defense Reutilization and Marketing Manual*, March 1990

DoDR 5200.1, *DoD Information Security Program,* 1997

JANAP-128*, Automatic Digital Network (AUTODIN) Operating Procedure*

AFPD 31-4, *Information Security*

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

AFPD 33-2, *Information Protection*

AFPD 38-5, *Unit Designations*

AFDIR 37-135*, Air Force Address Directory* (to become a data base)

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, Managing the Information Security Program

AFI 33-115, *Networks Management*

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

AFI 33-127, *Electronic Messaging Registration and Authority*

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

AFI 37-124, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections* (to become AFI 33-324)

AFMAN 33-128, *Electronic Messaging Registration*

AFMAN 37-126, *Preparing Official Communications* (to become AFMAN 33-326)

AFMAN 37-139, *Records Disposition Schedule* (to become AFMAN 33-339)

Abbreviations and Acronyms

AA—Approval Authority

ACP—Allied Communications Publication

ADUA—Administrative Directory User Agent

AF—Air Force (*used on forms only*)

AFI—Air Force Instruction

AFNCC—Air Force Network Control Center

AFPD—Air Force Policy Directive

AFSC—Air Force Specialty Code

AFSSI—Air Force Systems Security Instruction

AIG—Address Indicator Group

ALFOODACT—All Food Act

ALMILACT—All Military Activities

AMPE—Automated Message Processing Exchange

AOR—Area of Responsibility

ASC—AUTODIN Switching Center

AUTODIN—Automatic Digital Network

BITS—Base Information Transfer System

BMTA—Backbone Message Transfer Agent

CA—Certification Authority

CAW—Certification Authority Workstation

CM—Configuration Management

CNWDI—Critical Nuclear Weapon Design Information

COMPUSEC—Computer Security

COMSEC—Communications Security

CRC—Cycle Redundancy Check

CSP—Communications System Processor

CSSO—Computer Systems Security Officer

DBMS—Director Base Medical Services

DD—Department of Defense (used on forms only)

DIB—Directory Information Base

DII—Defense Information Infrastructure

DIREP—Difficulty Report

DISA—Defense Information Systems Agency

DISAC—Defense Information Systems Agency Circular

DISN—Defense Information Systems Network

DIT—Directory Information Tree

DMS—Defense Message System

DN—Distinguished Name

DoD—Department of Defense

DPC—Data Processing Center

DRU—Direct Reporting Unit

DSA—Directory System Agent

EAM—Emergency Action Message

ECP—Emergency Command Precedence

EWIR—Electronic Warfare Integrated Reprogramming

FOA—Field Operating Agency

FORTEZZA—PCMCIA card with NSA encryption algorithm

GCC—Global Control Center

GSM—Global Service Manager

HD—Help Desk

HQ AFCA—Headquarters Air Force Communications Agency

HQ SSG—Headquarters Standard Systems Group

HQ USAF—Headquarters United States Air Force

IAS—Immediate Access Storage

IMTA—Intermediate Message Transfer Agent

INSPECDIS—Inspector Distribution

IP—Information Protection

ITU-T—International Telecommunication Union-Telecommunication Standardization Sector

JANAP—Joint Army-Navy-Air Force Publication

LAN—Local Area Network

LCC—Local Control Center

LRU—Line Replaceable Unit

LSM—Local Service Manager

MAJCOM—Major Command

MC—Messaging Center

MCEB—Military Communications and Electronics Board

MFI—Multi-Function Interpreter

MISSI—Multilevel Information Systems Security Initiative

ML—Mail List

MLA—Mail List Agent

MML—Message Management Letter

MT—Message Terminal

MTA—Message Transfer Agent

MWS—Management Workstation

NCC—Network Control Center

NSA—National Security Agency

OF—Operational Form (*used on forms only*)

OI—Operating Instruction

O/R—Originator/Recipient

OPlan—Operations Plan

OPR—Office of Primary Responsibility

ORA—Organizational Registration Authority

ORI—Operational Readiness Inspection

PC—Personal Computer

PCMCIA—Personal Computer Memory Card International Association

PIN—Personal Identification Number

PLA—Plain Language Address

PM—Preventive Maintenance

PMO—Program Management Office

POC—Point of Contact

PUA—Profiling User Agent

RA—Registration Authority

RAYDAY—Radio Day

ROSC—Regional Operations and Security Center

RSM—Regional Service Manager

SA—System Administrator

SIOP-ESI—Single Integrated Operational Plan-Extremely Sensitive Information

SMTA—Subordinate Message Transfer Agent

SOP—Standard Operating Procedures

SPECAT—Special Category

SRA—Sub-Registration Authority

TCC—Telecommunications Center

TOC—Table of Contents

UA—User Agent

WGM—Workgroup Manager

Terms

Access Control—The methods that will allow only authorized personnel to use a computer system; in the defense message system, also the methods that allow only registered users to send or receive messages.

Accounting Management—The process of collecting, interpreting, processing, and reporting the cost of service information on which billing will be based.

Administrative Directory User Agent (ADUA)—A software function that provides the means whereby an authorized person can enter, modify, or delete data in the directory information base.

Approving Authority—The person who approves the appointment of the certification authority. Within the Air Force, HQ AFCA/GCI is the approving authority.

Architecture (of the Defense Message System [DMS])—The structure of DMS components, their interrelationships, and the principles and guidelines governing their design and evolution over time.

Availability—The probability that system functional capabilities are ready for use by a user at any time, where all time is considered, including operations, repair, administration, and logistic time.

Backbone Message Transfer Agent (BMTA)—The store-and-forward message switching component of the defense message system backbone.

Certification Authority Workstation (CAW)—A trusted workstation that is used only by the certification authority (CA). The CA is responsible for the defense message system directory maintenance in a given locality. 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.

Certification Authority (CA)—A person responsible for user certification, for placing certificates in the defense message system directory, and for programming FORTEZZA cards. The CA generates FORTEZZA cards using the CA workstation.

Component—In the defense message system, a software process or a combination of a software process and its hardware platform that performs a service in the preparation, transmission, or translation of messages.

Compromised Key List—A list of presumed compromised key identifiers. The format is defined by the responsible key management center.

Confidentiality—The property of a computer or communications system that ensures information is not made available or disclosed to unauthorized individuals, entities, or processes.

Configuration Management (CM)—A discipline applying technical and administrative direction and surveillance to: (a) identify and document the functional and physical characteristics of a configuration item, (b) control changes to those characteristics, and (c) record and report changes to processing and implementation status.

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

Defense Information Systems Network (DISN)—A sub-element of the Defense Information Infrastructure (DII), the DISN is the DoD's consolidated worldwide enterprise-level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations. It is transparent to its users, facilitates the management of information resources, and is responsive to national security and defense needs under all conditions in the most efficient manner.

Digital Signature—A non-forgeable transformation of data that allows proof of source, non-repudiation, and verification of data integrity.

Directory Information Base (DIB)—All of the information that exists in the directory system.

Directory—A collection of open systems cooperating to provide directory service. As used in this document, it refers specifically to the defense message system directory, based on the ITU-T X.500 recommendations.

Directory Information Tree (DIT)—A directory information base organizational model that employs a hierarchical tree structure.

Directory Service—A service of the external environment entity of the technical reference model that 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.

Directory System Agent (DSA)—The directory information base (DIB) in the DMS is distributed among a number of DSAs. Each of these contains a portion of the DIB, usually those portions most often needed by the users in the geographical area served by the DSA. The DSA is said to "master" the DIB portion normally assigned to it.

Directory User Agent (DUA)—The DUA communicates with the directory system agent to obtain directory information for its associated component.

Distinguished Name (DN)—A name that is unique. A directory DN is unique in the entire global directory; a relative DN is unique within a specific sub-tree.

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

Global Control Center (GCC)—The Defense Information Systems Agency global facility in Arlington, Virginia, that provides technical control and monitors the system and network integrity of the defense information infrastructure.

Global Service Manager (GSM)—The operations manager at the global level to provide operational control and management direction over the defense message system.

Help Desk (HD)—The primary point of contact 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.

Integrity—In messaging, the assurance that a message or other data has not been altered or destroyed in an unauthorized manner while in the messaging system.

Intermediate Message Transfer Agent (IMTA)—The store-and-forward message switching component of the defense message system (DMS), occupying a position in the DMS hierarchical architecture between the backbone message transfer agents (MTA) and the subordinate MTAs.

Legacy Systems—Current systems that do not comply with defense message system standards and have been identified for phase-out, upgrade, or replacement.

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.

Local Service Manager (LSM)—The operations manager for the local level who provides operational control and management direction over the defense message system at the base, camp, post, or station.

Mail List (ML)—A single message address that acts as a collective address. When a message originator transmits the message to a ML as the recipient name, a mail list agent is the address.

Mail List Agent (MLA)—A defense message system component that accepts messages addressed to mail lists (ML) and readdresses them to the individual recipients who are members of the ML.

Mail List Cognizant Authority—The command or activity assigned a mail list (ML) by the ML control authority. This is the organization for which the ML was established and which is authorized to transmit messages to the ML.

Mail List Control Authority—The service, agency, or organization responsible for the assignment and control of allocated mail lists.

Mail List Manager—A person who acts on behalf of a mail list cognizant authority to actually add, modify, or change a mail list in the directory.

Management Workstation (MWS)—The MWS is the primary tool for network management at all management levels. It has the capability of receiving, correlating, and distributing management information sent to it by the managed network components.

Message Store—The message store accepts messages from the message traffic system on behalf of the user agent (UA), and stores them until the UA returns to service.

Non-Repudiation—In a messaging system, any 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 Message—A message exchanged between organizational elements.

Organizational Registration Authority (ORA)—A local multi-level information systems security initiative administrative authority who assists a certification authority (CA) with registering end users by gathering end user registration information and forwarding it to the CA.

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

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.

Profiling User Agent (PUA)—A user agent who is capable of re-distributing a message according to its subject, contents, and key words.

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.

Radio Day (RAYDAY)—A telecommunications term used to represent message creation dates. The sequential day count of the days of a year, numbered sequentially from the first day of January (001 for 1 Jan, 002 for 2 Jan, etc.). Each RAYDAY begins at 0000 Greenwich mean time.

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

Regional Service Manager (RSM)—The operations manager for the region who provides operational control and management direction over the defense message system at the regional level.

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

Repudiation—The denial by a message originator or recipient that a message was sent or received. In the defense message system, the message signature ensures that an originator cannot repudiate the message.

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

Sub-Registration Authority (SRA)—The SRA assigns directory distinguished names and is responsible for registration matters 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.

Attachment 2

SUGGESTED ITEMS FOR LOCAL OPERATING PROCEDURES

A2.1. Temperature and Humidity Controls.

A2.2. Magnetic Media Controls.

A2.3. Management of the Remote Processing Facilities.

A2.4. Physical Security and Accountability.

A2.5. Duties of Equipment Custodian and Equipment Control Officer.

A2.6. Shift Activity and Turnover Log.

A2.7. Control of Difficulty Reports (DIREP) and Software Modification Reports.

A2.8. Power-Up or Power-Down Procedures. Clear with vendor engineer.

A2.9. Control and Distribution of System Advisory Notices and Difficulty Reports Status Reports.

A2.10. Housekeeping. Include cleaning schedules, methods, etc.

A2.11. Control and Handling of Systems Software Releases and Modifications. Include suspense dates. Furnish for necessary advice and distribution to functional users.

A2.12. Classified Processing. Include disconnect procedures for remote terminals (including dial-ups), marking, control, storage, and disposal of input, output, and waste.

A2.13. Personal Data Subject to the Privacy Act of 1974.

A2.14. Internal Training. Appoint an on-the-job training monitor, as required.

A2.15. Maintenance of Automatic Data Processing Equipment.

A2.16. System Initialization Procedures.

A2.17. Severe Weather Conditions.

A2.18. Production Distribution Center.

A2.19. Products Requiring Special Handling (e.g., payroll checks, SPECAT, classified, high precedence, etc.).

A2.20. Time Checks.

A2.21. Procedures and Analysis Function.

A2.22. Customer Education and Support. Include customer visits and customer satisfaction surveys.

A2.23. Service Messages.

A2.24. Message Tracer Action.

A2.25. Unit Computer Systems Security Officer and Terminal Area Security Officer Duties.

A2.26. Procedures for the Control of Remote Terminal Access (to include dial-ups). Also include password generation, distribution, and control.

A2.27. Status Reporting.

A2.28. Service Calls for Maintenance.

A2.29. Contingency and Catastrophic Failures. Facility emergency plans cover:

A2.29.1. Alert or recall.

A2.29.2. Protection or disposal of classified information and equipment.

A2.29.3. Fire emergency and prevention.

A2.29.4. Site environmental failure.

A2.29.5. Identification of emergency reporting.

A2.29.6. Bomb threats.

A2.29.7. Evacuation.

A2.30. Duties of the Database Administrator Functions. Include transaction interface processor management, network management, and data base management.

A2.31. Local System Security Incident Reporting. Include unsuccessful attempts to access the system, erasure or destruction of stored data, etc.

A2.32. Automated and Manual Audit Trails. Include minimum actions recorded, checking, and retention.

A2.33. Marking and Control of Programs.

A2.34. Off-Site Storage. Include security, environment, storage, updating, and inventory procedures.

A2.35. Duties of the Magnetic Storage Librarian Function.

A2.36. Duties and Responsibilities of Shift Supervisor or Leader.

A2.37. System Backup Procedures.

A2.38. Performance Management.

A2.39. Configuration Management.

Attachment 3

SAMPLE MEMORANDUM-DESIGNATION OF PREVENTIVE MAINTENANCE

A3.1. Develop a written agreement for contractor maintained equipment. You may use this sample memorandum.

MEMORANDUM FOR (*Vendor, Local Branch Address*)

FROM:

SUBJECT:Preventive Maintenance Schedule and Designation of Principal Period of Maintenance,

(*Vendor/GSA Contract Number*)

1. Reference (*paragraph or article*), (*special item or section*), subject contract, with regard to maintenance of data processing equipment.

2. Effective (*date*), the principal period of maintenance for this installation is established as (*hours of the day and days of the week*). The vendor will perform preventive maintenance on the equipment listed on delivery orders (*numbers and date*), or as listed here, beginning at (*time of day*) and ending at (*time of day*) on (*days*) of each week.

3. Mutual agreement to this schedule is indicated below.

FOR THE AIR FORCE

(*Signature of Equipment Control Officer*)

FOR (Vendor)

(*Signature of Vendor Representative*)

Attachment 4

SOFTWARE DEFICIENCY REPORT

A4.1. The reporting requirements in this attachment are exempt from licensing according to AFI 37-124, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Inter-Agency Air Force Information Collections* (to become AFI 33-324).

A4.2. Categories of Deficiencies.

A4.2.1. Category 1 Problem. An on-line program problem that seriously jeopardizes traffic handling capability or impairs system integrity. Generally, problems assigned this classification involve those which reduce the system capability for maintaining message integrity, create security or lost message hazards, generate on-line or off-line duplicate messages, and cause computer failures that stagnate traffic.

A4.2.2. Category 2 Problem. A program problem that affects the on-line system. However, it does not jeopardize traffic handling or impair system integrity. Normally, Category 2 problems involve situations and conditions that create an additional workload on system operations but do not warrant immediate relief.

A4.2.3. Category 3 Problem. Any program problem which affects off-line operations, excluding off-line recovery problems that fall under Category 1 criteria.

A4.2.4. Category X Problem. This category is reserved for those problems that are unidentifiable as Category 1, 2, or 3. Usually, such problems will be resolved by determination of specifications, documentation changes, procedural changes, change to operator error and closed, or removed as a problem and submitted by the originating agency as a recommended enhancement for those areas that involve elimination of operator problems or irritants.

A4.2.5. The following is an example of an operational software deficiency report for Categories 2, 3, and X:

FROM: OPERATING UNIT COMMANDER OR OPERATIONS OFFICER

TO: OPERATING UNIT'S HEADQUARTERS

INFO: HQ ESC HANSCOM AFB MA//CV//

HQ SSG MAXWELL AFB GUNTER ANNEX AL//DGI/DGIC//

HQ AFCA SCOTT AFB IL//GCOM//

DIRUSAISSDC-H FT HUACHUCA AZ//ASQBI-HSA//(*standard remote terminal [SRT] system only*)

HQ AIA KELLY AFB TX//IND//(*communications system processor [CSP] system only*)

(*Other applicable addressees using similar systems, if appropriate*)

(*CLASSIFICATION*)

SUBJECT: OPERATIONAL SOFTWARE DEFICIENCY REPORT

REQUEST YOU TAKE ACTION TO ANALYZE AND RESOLVE THE FOLLOWING SUSPECTED OPERATIONAL SOFTWARE DEFICIENCY:

A. COMPUTER SYSTEM TITLE:

B. DEFICIENCY PRIORITY: (*2,3, and X ROUTINE*)

C. EXPLANATION OF DEFICIENCY:

D. RECOMMENDATION FOR RESOLUTION OF DEFICIENCY:

E. REMARKS: (*equipment types, coordination affected, etc.*)

F. NAME, GRADE, PHONE NUMBER, AND TITLE OF ACTION OFFICE.

A4.2.6. The following is an example of an operational software deficiency report for Category 1:

FROM:OPERATING UNIT COMMANDER OR OPERATIONS OFFICER

TO:DIRUSAISSDC-H FT HUACHUCA AZ//ASQBI-HSA//

HQ AIA KELLY AFB TX//IND//(*CSP systems only*)

HQ ESC HANSCOM AFB MA//CV//

INFO: HQ SSG MAXWELL AFB GUNTER ANNEX//DIG/DIGC//

HQ AFCA SCOTT AFB IL//GCOM//

OPERATIONAL UNIT'S MAJCOM/DRU/FOA HEADQUARTERS

(Other applicable addressees using similar systems if appropriate)

(*CLASSIFICATION*)

SUBJECT: OPERATIONAL SOFTWARE DEFICIENCY REPORT

REQUEST YOU TAKE ACTION TO ANALYZE AND RESOLVE THE FOLLOWING SUSPECTED OPERATIONAL SOFTWARE DEFICIENCY:

A. COMPUTER SYSTEM TITLE:

B. DEFICIENCY PRIORITY: (*Emergency*)

C. EXPLANATION OF DEFICIENCY:

D. RECOMMENDATION FOR RESOLUTION OF DEFICIENCY:

E. REMARKS: (*equipment types, coordination affected, etc*.)

A4.2.7. The following is an example of an operational software implementation notice (**NOTE:** Notices submitted to close reported deficiencies not adequately documented, have not recurred within 30 days, or not recreated, have as their subject "Deficiency Closure Notice" and written to describe the "Computer System Title," the "Deficiency Number Closed," and the explanation that the "Deficiency has not recurred for 30 days and was not recreated."):

FROM: OPERATING UNIT COMMANDER OR OPERATIONS OFFICER

TO: DIRUSAISSDC-H FT HUACHUCA AZ//ASQBI-HSA//

HQ AIA KELLY AFB TX//IND//(*CSP systems only*)

HQ ESC HANSCOM AFB MA//CV//

HQ SSG MAXWELL AFB GUNTER ANNEX AL//DIG/DIGC//

INFO: HQ AFCA SCOTT AFB IL//GCOM//

OPERATIONAL UNIT'S MAJCOM/DRU/FOA HEADQUARTERS

(*Other applicable addressees using similar systems, if appropriate*)

(*CLASSIFICATION*)

SUBJECT: OPERATIONAL SOFTWARE IMPLEMENTATION NOTICE

OPERATIONAL SOFTWARE WAS SUCCESSFULLY IMPLEMENTED AND DETAILS ARE AS FOLLOWS:

A. COMPUTER SYSTEM TITLE:

B. SOFTWARE IDENTIFICATION: (*software configuration designator*)

C. JULIAN DATE AND TIME IMPLEMENTED:

D. DEFICIENCY NUMBER CLOSED:

E. REMARKS: (*equipment types, coordination affected, etc.*)

Attachment 5

QUESTIONS FOR DEVELOPING A MESSAGING AND DATA PROCESSING CENTERS MANAGEMENT CHECKLIST

A5.1. Major Commands (MAJCOM), Direct Reporting Units (DRU), and Field Operating Agencies (FOA).

A5.1.1. Has the parent MAJCOM/FOA/DRUs established local operational policies and procedures, including transitional planning? (paragraph 1.4.2)

A5.1.2. Does the communications and information processing equipment and personnel meet the needs of the users? (paragraph 1.4.3)

A5.1.3. Were traffic analysis standards or other measurements established to evaluate performance according to local procedures? (paragraph 1.4.5)

A5.2. Messaging Centers.

A5.2.1. Do network control centers (NCC) configure and audit security logs for defense message system (DMS) components (*NCCs only*)? (paragraph 1.5.2)

A5.2.2. Was a local configuration management database prepared and updated? (paragraph 1.5.3)

A5.2.3. Was a help desk service (customer service) established to resolve user problems and concerns? (paragraph 1.5.7)

A5.2.4. Were local alternate routing procedures established to ensure high priority users have the capability of establishing associations with at least two subordinate message transfer agents (SMTA)? (paragraph 1.5.9)

A5.2.5. Are procedures in-place to coordinate base connectivity interruptions to the DMS infrastructure with the servicing regional operations and security center (ROSC)? (paragraph 1.5.10)

A5.2.6. Is a station log maintained to record significant events? (paragraphs 1.5.11 and 3.5)

A5.2.7. Were local procedures for notification of MINIMIZE established? (paragraph 1.5.12)

A5.2.8. Are all DMS system and equipment changes coordinated with the DMS-Air Force Program Management Office (AF PMO) and the Defense Information Systems Agency (DISA) (*NCCs only*)? (paragraph 1.5.14)

A5.2.9. Is an on-the-job training program maintained? (paragraph 1.5.17)

A5.2.10. Was a customer education program established? (paragraph 1.5.18)

A5.2.11. Do destruction facilities meet the needs of the messaging center (MC) and data processing center (DPC)? (paragraph 1.5.19)

A5.2.12. Are the support agreements for all tenants staffed and coordinated IAW AFI 25-201? (paragraph 1.5.20)

A5.2.13. Were sub-registration authorities (SRA), organizational registration authorities (ORA), and mail list (ML) control authorities(CA) appointed (*NCCs only*)? (paragraph 1.5.22)

A5.2.14. Was an immediate access storage manager appointed for each installed computer system? (paragraph 1.5.24)

A5.2.15. Has the NCC assigned a system agency (SA) for each DMS component (*NCCs only*)? (paragraph 1.6)

A5.2.16. Were personal encrypted computer memory cards (FORTEZZA) requested for all DMS components (*NCCs only*)? (paragraph 1.6.4)

A5.2.17. Are system backups and recoveries performed? (paragraph 1.6.7)

A5.3. Messaging Users.

A5.3.1. Are security policies in-place for safeguarding both FORTEZZA card and personal identification number (PIN)? (paragraph 1.7.2)

A5.3.2. Are directory searches limited, based on local policy? (paragraph 1.7.5)

A5.3.3. Are messages and information protected under the Privacy Act? (paragraph 1.7.7)

A5.3.4. Were procedures established to control and prevent tampering of messages being sent and received? (paragraph 1.7.8)

A5.4. Messaging Center and Data Processing Center Facility Management.

A5.4.1. Were safety and fire practices and procedures set up? (paragraph 2.2)

A5.4.2. Were contingency operations plans developed? (paragraph 2.5)

A5.4.3. Was a preventive maintenance schedule for all equipment established? (paragraph 2.6)

A5.5. Messaging Center and Data Processing Center Operations Management.

A5.5.1. Are procedures in-place for operating computer equipment during severe weather conditions (such as thunderstorms within 10 statute miles of an installation, ice storms, high wind conditions, etc.) including contractual liabilities for unique systems? (paragraph 3.2)

A5.5.2. Were local procedures for alternate routing of messaging traffic set up? (paragraph 3.3)

A5.5.3. Are procedures in-place to ensure Automatic Digital Network (AUTODIN) address indicator group (AIG) and DMS ML case files remain current at all times? (paragraph 3.6)

A5.5.4. Are local procedures for MINIMIZE established (ACP 121)? (paragraph 3.8)

A5.5.5. Are software deficiency reports used to identify problems? (paragraph 3.10)

A5.5.6. Are local procedures developed for quarterly customer visits and user group meetings? (paragraph 3.11)

A5.5.7. Were customer education programs or questionnaires developed to ensure customer requirements are met and the mission requirement is fully supported? (paragraph 3.11)

A5.6. Messaging Center and Data Processing Center Software Processing.

A5.6.1. Do units notify the software support office when a software upgrade is implemented? (paragraph 4)

A5.6.2. Are the parent MAJCOM, FOA, DRU, HQ SSG/SIDI, and HQ SSG/DIGC addressed on all DMS deficiency processing correspondence? (paragraph 5.1)

A5.6.3. Do units notify the applicable software support office of software patch within 24 hours of patch implementation? (paragraph 5.3)

A5.7. Messaging Center and Data Processing Center Message Handling.

A5.7.1. Is AUTODIN use limited to official business that cannot be sent by other forms of electrical transmission? (paragraph 6.1)

A5.7.2. Do message originators and releasing authorities review all messages to ensure those not meeting MINIMIZE requirements are sent by other than electrical means? (paragraph 6.2.3.2)

A5.7.3. Are current message management letters on file at the MC? (paragraph 7.1.4)

A5.7.4. Is the base information transfer system (BITS) or the base network (e-mail) used to deliver messages not requiring special handling? **NOTE:** Do not send classified messages over unsecure networks. (paragraph 7.1.8)

A5.7.5. Are general messages tracked chronologically for the current year? (paragraph 7.1.18)

A5.7.6. Are local office symbol addresses filed with the customer-provided list of AIG local addresses? (paragraph 7.1.19)

A5.7.7. Are message management letters (MML) updated quarterly? (paragraph 7.1.20)

A5.8. Outgoing Message Processing.

A5.8.1. Is information protected against loss or compromise? (paragraph 7.2.1)

A5.8.2. Are all diskettes scanned for viruses? (paragraph 7.2.13)

A5.9. Storage Media Management.

A5.9.1. Are procedures set up to cover control, security, and upkeep of all storage media? (paragraph 9.1)

A5.9.2. Are library inventory accountability records available that provide listings of the media on hand, 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? (paragraph 9.3)

A5.9.3. Are disk management standards governing programs and files allowed to reside on disks set up? (paragraph 9.4.2.1)

A5.9.4. Are backup critical programs, disk resident files, system software routines, production programs, and data files on tape and stored in a secure location away from the facility? (paragraph 9.4.2.3)

A5.10. Architecture and Staffing.

A5.10.1. Has the NCC developed strategies to eventually physically consolidate the telecommunications center (TCC) and NCC upon elimination of the legacy AUTODIN TCCs? (paragraph 10.1.2)

A5.10.2. Are NCC Help Desk (HD) personnel familiar with the operations, management, security services, and directory services of the DMS? (paragraph 10.1.4)

A5.11. Directory Shadowing.

A5.11.1. Are shadow directory information bases (DIB) updated from the master within 10 minutes of a change to the master? (paragraph 10.3)

A5.11.2. Has each activity maintaining a global-level DSA established a shadowing agreement with at least one other global-level DSA? (paragraph 10.3.1)

A5.11.3. Has each activity maintaining a local-level DSA established a shadowing agreement with at least one other local-level DSA? (paragraph 10.3.2)

A5.11.4. Does the Annex K to the operations plan (OPlan) contain directory shadowing procedures?

(paragraph 10.3.3)

A5.12. Defense Message System System Backups.

A5.12.1. Are daily incremental backups kept for 1 weekly backup cycle? (paragraph 11.1.1)

A5.12.2. Are weekly full backups retained for two cycles? (paragraph 11.1.2)

A5.12.3. Are the weekly full backups rotated to an off-site location? (paragraph 11.1.3)

A5.12.4. Were the original copies of all DMS software and operating system programs sent to the off-site location? (paragraph 11.1.4)

A5.13. Network Control Center Help Desk.

A5.13.1. Has the HD provided customer education on message trace procedures? (paragraph 11.2.1)

A5.13.2. Do message trace requests contain the user's message identification information, the recipients of the message, and the time of submission? (paragraph 11.2.2)

A5.13.3. Are trouble tickets used to document trace requests? (paragraph 11.2.3)

A5.13.4. Are message originators notified of the final results of the trace action? (paragraph 11.2.4)

A5.14. Message Retention.

A5.14.1. Are all messages originated, stored, or received in DMS maintained in accordance with AFMAN 37-139 (to become AFMAN 33-339)? (paragraph 11.3)

A5.14.2. Are on-line audit trails and logs accessible within 10 minutes, and off line records within 4 hours? (paragraph 11.3.1)

A5.14.3. Are all incoming and outgoing messages stored at the user component for a minimum of 10 days? (paragraph 11.3.2)

A5.15. Alternate Routing/Delivery Points.

A5.15.1. Have organizational user accounts not manned on a 24 hour, 7 day basis (24/7) arranged for an alternate delivery point for high-priority traffic when not manned? (paragraph 11.4.1)

A5.15.2. Have DMS clients who are not manned 24/7, implemented an auto-forward capability to ensure delivery of URGENT messages to a 24/7 point of contact (POC)? (paragraph 11.4.4)

A5.16. Defense Message System Mail List Management.

A5.16.1. Are MLs used for organizational messaging? (paragraph 12.1)

A5.16.2. Are MLs shared between organizations when appropriate? (paragraph 14.2.1)

A5.16.3. Is justification provided when ML compositions and purposes are duplicated? (paragraph 14.2.2)

A5.16.4. Are obsolete MLs deleted, and was the control authority, the ML manager, and the ML members notified of the deletion? (paragraph 14.2.8)

A5.16.5. Are ML create, change, and delete actions performed within 3 days after notification from the cognizant authority? (paragraph 15.1)

A5.16.6. Was a FORTEZZA card obtained for the mail list agent (MLA)? (paragraph 15.2)

A5.16.7. Are references ("backpointers") from the ML member entry to the ML entry maintained? (paragraph 15.4)

A5.16.8. Does the ML manager keep a current list of all ML assignments with related ML information? (paragraph 15.10)