



CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6

DISTRIBUTION: A, B, C, J, S

CJCSI 5721.01A

1 May 1999

THE DEFENSE MESSAGE SYSTEM AND ASSOCIATED MESSAGE PROCESSING SYSTEMS

REFERENCES: See Enclosure C.

1. Purpose. This instruction provides policy, guidance, and information regarding the use, operation, and management of the Defense Message System (DMS).
2. Cancellation. CJCSI 5721.01, 28 June 1993, is canceled.
3. Applicability. This policy applies to all Defense agencies responsive to the Chairman of the Joint Chiefs of Staff, Services, and combatant commands in planning, managing, and using organizational and individual message processing systems that compose DMS messaging.
4. Policy
 - a. Policy outlined in this instruction supports the DMS goal of evolving to new technology, while reducing costs and staffing and maintaining levels of AUTODIN service and security. The DMS Implementation Plans developed by the Services and Defense agencies describe the transition from AUTODIN to DMS messaging.
 - b. Policy pertaining to organizational (formal) message processing systems, including AUTODIN and its direct and indirect connected subscribers, is contained in Enclosure A.
 - c. Policy pertaining to individual message processing systems that communicate using the Defense Information Systems Network (DISN) is contained in Enclosure B.
 - d. DOD policy is to acquire and use products or services that are compliant with the Joint Technical Architecture (JTA), Defense

1 May 1999

Information Infrastructure Common Operating Environment (DII COE), Base Information Infrastructure (BII) and/or DISN long-haul communications equipment and services effectively, efficiently, and economically.

e. The host Military Department (MILDEP)/agency should provide tenants on bases, posts, camps, or stations (BPCS) common user voice, internet protocol (IP) router, and application layer message handling services (e.g., DMS). Local host/tenant agreements or inter-Service support agreements may include cost recovery where appropriate.

5. Definitions. None.

6. Guidance

a. The DMS management structure provides program oversight and execution, planning, security policy, architecture, and administrative controls related to the DMS program objectives.

b. DISA and the Joint Interoperability Test Command (JITC), as the independent test organization for DMS, ensure DMS operates as an integrated system, especially for high-assurance organizational messaging. Developmental, integration, and operational testing processes are outlined in the DMS Capstone Test and Evaluation Master Plan (TEMP) reference a.

c. DISA will provide operational management of all DMS infrastructure products that have been implemented following DMS product deployment approval.

d. The Director, Intelligence Community DMS Management Office (ICDMO), as directed by the Intelligence Systems Board, will perform the day-to-day management of the Special Compartmented Information (SCI) portion of DMS.

7. Responsibilities

a. Each Service and Defense agency has developed DMS transition plans that include plans, projects, products, and related implementation schedules.

(1) These plans support the objectives of DMS, to include reducing costs and staffing while meeting or exceeding current levels of service and security.

1 May 1999

(2) The DMS transition plan of supporting organizations must reflect pertinent information when a Service or Defense agency provides message processing support or sponsors other activities, including combatant commands or non-DOD and non-US subscribers.

b. Approval requirements for non-DOD and non-US activities use of DMS are in Enclosure A.

c. DISA schedules and approves transition plans and amendments in conjunction with appropriate elements of the DMS management structure.

8. Summary of Changes. This change:

a. Added reference to DOD policy on use of BII and DII.

b. Updated SCI responsibilities.

c. Deleted references to GOSIP and the DMS Component Approval Process (CAP).

d. Added reference to the DMS Capstone Test and Evaluation Master Plan as a replacement for the DMS Compliance, Test, and Evaluation (CT&E) Plan.

e. Update reference to the DMS Multicommand Required Operational Capabilities (MROC).

f. Added references to the DOD Information Technology Security Certification and Accreditation Process (DITSCAP) as a replacement for the DMS Component Approval Process (CAP).

9. Releasability. This instruction is approved for public release; distribution is unlimited. DOD components (to include the combatant commands), other Federal agencies, and the public may obtain copies of this instruction through the Internet from the CJCS Directives Home Page--<http://www.dtic.mil/doctrine/jel/cjcsd.htm>. Copies are also available through the Government Printing Office on the Joint Electronic Library CD-ROM.

10. Effective Date. This instruction is effective upon receipt.

For the Chairman of the Joint Chiefs of Staff:

A handwritten signature in black ink, appearing to read 'S. Rippe', with a stylized flourish extending to the right.

STEPHEN T. RIPPE
Major General, USA
Vice Director, Joint Staff

Enclosures:

- A -- Organizational Messaging Policy
- B -- Individual Messaging Policy
- C -- References
- GL -- Glossary

DISTRIBUTION

Distribution A, B, C, and J plus the following:

	<u>Copies</u>
Commander, US Element NORAD.....	2
Director, Joint Interoperability Test Center.....	2
Chairman, Inter-American Defense Board.....	2
Chairman, US Section, Military Cooperation Committee.....	2
USNMR to SHAPE.....	2
USREPMC Liaison Office.....	2
USLO to SACLANT.....	2
Chairman, ICDMO.....	2

(INTENTIONALLY BLANK)

ENCLOSURE A

ORGANIZATIONAL MESSAGING POLICY

1. DMS Description. DMS is an applications layer messaging system that relies on the DISN for its transport. It consists of all hardware, software, procedures, standards, facilities, and personnel used to exchange messages electronically between DOD organizations and individuals in a fixed location or tactical environment. DMS also supports messaging for allied systems. DMS requirements are in reference b.
2. DMS Infrastructure
 - a. General
 - (1) AUTODIN
 - (a) Meets all requirements of reference b -- connectivity and interoperability, message delivery, timely delivery, confidentiality and security, sender authentication, message integrity, availability and reliability, training, recipient identification, message preparation support, storage and retrieval support, and distribution determination and delivery.
 - (b) Will continue to support organizational message users until they are transitioned to DMS. Current mandate is that AUTODIN be phased out by 31 December 1999.
 - (2) DMS Transition Hubs (DTH)
 - (a) Are being commissioned in FY 1999 to provide legacy switching functionality and translation services.
 - (b) Provide ruthless preemption capability, primarily for the Emergency Action Message (EAM) dissemination community through the legacy switching portion.
 - (c) Will remain operational and be sustained at the necessary level to satisfy requirements of reference b.
- 1 The connection approval process for remaining connected to DTHs (vice transitioning to DMS) is described in reference c. ASD

1 May 1999

(C3I), with Joint Staff (J6T) recommendation, is the approving authority for DTH direct connections.

2 Emergency Action Messages (EAMs) dissemination support is the primary justification for retaining a DTH connection.

(3) DMS multifunction interpreters (MFI) provide translation services between DMS and legacy message format users. MFIs are clustered at the DTHs to take advantage of personnel and facilities with extensive AUTODIN experience.

(4) DMS is an evolutionary program. A tightly integrated system is required to meet organizational messaging requirements outlined in the MROC (reference b). The DMS TEMP will ensure that these products satisfy high-grade, high-assurance requirements of reference b.

(5) ASCs will be phased out IAW reference c.

b. Authorities. Reference d is the applicable authority.

(1) The Director, DISA, will exercise program management oversight, system design, engineering, acquisition, implementation, integration, operational direction, and management control over all elements of the DMS as a DII component.

(2) The Commander, JITC, will administer DMS developmental, integration and operational testing.

(3) Security approvals, in accordance with the DMS Capstone TEMP, will be the joint responsibility for designated approving authorities (DAAs):

(a) NSA for products handling critical communications information.

(b) DIA for products handling SCI information.

(c) DISA for products handling General Service (GENSER) information, not including Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI).

(d) Joint Staff/DJS for products handling SIOP-ESI information.

1 May 1999

c. Security. Reference e is applicable. Security protection is required for all messaging products at all classification levels. DMS messages will be protected by NSA-approved security protection mechanisms. Overall adequacy of security protection is determined for each DMS product by the DAAs (as described in 2(b) above) through DMS testing procedures.

d. AUTODIN Bridging

(1) Users directly connected to DTHs will remain on a discrete network and will not connect to DISN, other wide-area networks, or local area networks. However, legacy message format processing systems may connect to such networks, establishing a bridge to or from AUTODIN, or to facilitate the translation of legacy formats and the transition of legacy systems to DMS or other means.

(2) To ensure that DMS integrity and security of message traffic is protected, bridging systems will be identified when they are submitted to DISA for approval through DITSCAP (See reference f). Previously approved DMS or AUTODIN products that are being modified in a manner that results in a bridging configuration will also be submitted for DITSCAP approval.

(3) In the DOD Intelligence Information System (DODIIS) community, for SCI, the bridging and architecture are detailed in reference g.

e. DMS User Components

(1) Product (Component) Deployment. DMS user products, to include DTH equipment and connections to the SECRET Internet Protocol Router Network (SIPRNET), must obtain product deployment approval via the DITSCAP. Once fielded, the operating activity must respond to DISA reporting requirements and traffic management instructions. User products are defined in reference h.

(2) Accreditation and Security Oversight

(a) Each Service and agency operating a DMS GENSER user product will accredit that product, ensuring that all DITSCAP requirements are met, including DAA security approval.

(b) Accreditation of DMS implementation on SCI networks will be IAW reference i and applicable Department and agency procedures for certification and accreditation of SCI systems.

1 May 1999

(c) The Joint Staff, Services, joint agencies and commands are sole authorities for determining users with a need to process SIOP-ESI messages (See reference j). The Director, Joint Staff, is the DAA for all SIOP-ESI accreditation; however, J-38 is the executive agent for all Joint Staff DAA actions.

(3) Security. Implementers must comply with reference i as applicable. Adequacy of security protection is determined for each DMS product by DAAs and Service and agency accreditors through DITSCAP procedures.

(4) Tactical. IAW MROC, Change 1, DMS will support the tactical community. DMS will be extended into an area of operations to respond to validated operational requirements. Tactical communications equipment may be used at the direction of the commander of a unified or joint force command to provide the extension.

(5) Automated Message Processing Exchange (AMPE). AMPEs have been targeted for early elimination during the DMS evolution. Accordingly, all Services and agencies will expedite AMPE replacement. Replacement projects for AMPE and resulting components will meet the DMS objective to reduce costs and staffing, meet or exceed current standards of service, be in consonance with the DMS architecture, and satisfy the DITSCAP deployment approval requirements.

(6) Data Pattern Message Processing Systems. All data pattern traffic will be eliminated from the baseline DMS. Data pattern traffic consists of messages that use actual card medium (80 columns with language media format CC) or magnetic tape medium (variable length with language media formats BB, DD, and II). It does not include card image format, used by most personal computer messaging systems, nor does it include other applications of the CC language media format used to transmit narrative messages. Services and agencies, in conjunction with DISA and DMS management, will determine and use alternative means for transmitting and processing affected data pattern traffic.

(7) Telecommunications Centers. TCCs will be replaced by message processing products that eliminate paper deliveries by providing writer-to-reader electronic service that meets DMS objectives and architecture. Requirements of reference b are applicable to all end users.

3. DMS Services for Non-DOD Activities

a. US Government non-DOD activities may be considered for DMS services, upon OSD approval, if any of the following conditions exist:

- (1) The requirement is considered command and control and cannot be satisfied by other means.
- (2) The requirement directly or indirectly supports a DOD mission.
- (3) Other justification is deemed appropriate by OSD.

b. US non-Government activities may be considered for DMS services, upon OSD approval, if any of the following conditions exist:

- (1) They are sponsored by a DOD activity.
- (2) Their requirement is in direct support of a DOD mission.
- (3) Other justification is deemed appropriate by OSD.

c. Non-US activities may be considered for DMS services. Their requests will be processed under the provisions of reference k, and approved by OSD. As appropriate, OSD will direct DISA to effect or facilitate implementation.

4. DMS Transition Plan for Non-DOD Activities. DISA will take action through the DMS management structure to ensure that all non-DOD, non-Government, and non-US activities are notified of DMS planning. In particular, DISA will ensure that non-DOD activities currently receiving baseline services are addressed in all aspects of the DMS transition planning.

(INTENTIONALLY BLANK)

ENCLOSURE B

INDIVIDUAL MESSAGING POLICY

1. Electronic mail (E-mail), including all local area network-based and host-based messaging services, will migrate to DMS-compliant protocols. Implementation of SDA Flexible Design Architecture will be IAW approved Service and agency DMS transition plans.
2. Previously installed non-DMS-compliant solutions may coexist during the DMS transition and will be converted to DMS-compliant systems. A clearly documented strategy to migrate each proprietary system to full DMS compliance will be developed and maintained by DISA.
3. The Director, DISA, will provide additional implementation guidance to Services and Defense agencies and initiate DMS compliance certification. The Intelligence System Board may provide additional implementation guidance to Services, Defense agencies, and US Government non-DOD agencies using DMS on SCI networks.
4. Procedural instructions will be included in implementation guidance provided by DISA.

(INTENTIONALLY BLANK)

ENCLOSURE C

REFERENCES

- a. "Defense Message System (DMS) Revised Capstone Test and Evaluation Master Plan (DMS TEMP)", 8 September 1998
- b. MCM 20-89, 31 October 1997, "Defense Message System."
- c. "DOD Automatic Digital Network (AUTODIN) Switching Center (ASC) Phase-out and Defense Message System (DMS) transition Hub (DTH) Implementation Master Plan," 9 September 1998
- d. DOD Directive 5105.19, 25 June 1993, "Defense Information Systems Agency (DISA)"
- e. DOD Directive 5200.28, 21 March 1988, "Security Requirements for Automated Information Systems (AISs)"
- f. DOD 5200.40, 30 December 1997, "DOD Information Technology (IT) Security Certification and Accreditation (C&A) Process (DITSCAP)"
- g. DOD Intelligence Information System (DODIIS) Community AUTODIN Bypass Concept of Operations (CONOPS), 19 November 1998
- h. Assistant Secretary of Defense (C4I) memorandum, 18 October 1996, "Policy Guidance for Defense Message System (DMS) Implementation, Operation, and Life-Cycle Management (LCM)"
- i. DCI Directive 1/16 (SECRET), 19 July 1988, "Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks (U)"
- j. CJCSI 3231.01, 30 November 1993, "Safeguarding the Single Integrated Operational Plan"
- k. CJCSI 6740.01, 30 August 1996, "Military Telecommunications Agreements and Arrangements Between the United States and Regional Defense Organizations or Friendly Foreign Nations"

(INTENTIONALLY BLANK)

GLOSSARY

PART I -- ABBREVIATIONS AND ACRONYMS

AMPE	Automated Message Processing Exchange
ASC	AUTODIN Switching Center
AUTODIN	Automatic Digital Network
BII	Base Information Infrastructure
BPCS	base, post, command, station
C&A	Certification and Accreditation
CAP	Component Approval Process
COE	Common Operating Environment
CT&E	Compliance, Test, and Evaluation
DAA	Designated Approval Authority
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DISN	Defense Information System Network
DITSCAP	DOD Information Technology Security Certification and Accreditation Process
DODIIS	DOD Intelligence Information System
DTH	DMS Transition Hub
EAM	Emergency Action Message
E-Mail	Electronic Mail
GENSER	General Service
GOSIP	Government Open Systems Interconnecting Profile
ICDMO	Intelligence Community DMS Management Office
IP	Internet Protocol
JTA	Joint Technical Architecture
JITC	Joint Interoperability Test Command
MFI	Multifunction Interpreter
MILDEP	Military Department
MLA	Mail List Agent

MROC	Multicommand Required Operational Capability
MTA	Message Transfer Agent
NSA	National Security Agency
PUA	Profiling User Agent
SCI	Special Compartmented Information
SDA	System Design Architecture
SIOP-ESI	Single Integrated Operations Plan- Extremely Sensitive Information
SIPRNET	Secret Internet Protocol Router Network
TEMP	DMS Capstone Test and Evaluation Master Plan
TCC	Test Control Center