CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6 CJCSI 5721.01E
DISTRIBUTION: A, B, C, JS-LAN, S 13 August 2010

THE DEFENSE MESSAGE SYSTEM AND ASSOCIATED LEGACY MESSAGE PROCESSING SYSTEMS

References: See enclosure C.

1. Purpose. This instruction provides policy, guidance, responsibilities, and information regarding the use, operation, and management of the Defense Message System (DMS).

2. Cancellation. CJCSI 5721.01D, 8 February 2008, 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, operating, managing, and using message processing systems that comprise the DMS. This instruction is available to non-DOD U.S. agencies and allied organizations for information.

4. Policy

a. The policy and guidance outlined in this instruction support taking full advantage of new and evolving technology.

b. Policies pertaining to organizational message definition and processing, U.S. Message Text Format (USMTF), and National Gateway Centers (NGCs) are contained in Enclosure A.

c. Guidance pertaining to organizational messaging, messaging architecture, and implementation parameters are contained in Enclosure A.

d. Non-DOD and non-U.S. activities requesting use of U.S. messaging systems and their functionality must apply in accordance with the processes outlined in Enclosure A and reference a.

e. In recognition that it may be in the national interest to share classified military information (CMI) with foreign nations, the National Security Council, with approval of the President, established a national policy, National Disclosure Policy-1 (NDP-1) (reference b), governing disclosure of CMI to foreign governments. Disclosure of CMI to foreign governments and international organizations is limited and is in accordance with NDP-1 and reference c.

5. Definitions

a. Organizational Message. Organizational messaging includes command, control, communications, computers, and intelligence message exchange between organizational elements. The following are characteristics of organizational messages:

(1) Require approval for transmission by a designated official and determination of internal distribution by the receiving organizations.

(2) Are directive in nature, commit resources, make formal requests and/or provide command position.

(3) Must be auditable and/or traceable, provide for non-repudiation, and be subject to confidentiality and mandatory and discretionary access control protections.

(4) Must be signed and encrypted from the time of release.

b. National Gateway Center. The NGC ensures messaging interoperability with allies, coalition partners, non-DOD U.S. agencies, and other non-DOD U.S. and foreign organizations (e.g., U.S. defense contractors).

c. Individual Messaging. Includes working communications between individual DOD personnel within administrative channels, both internal and external to the specific organizational element, including non-DOD users. Such messages do not commit or direct an organization. Individual messages do not require the same level of system management, priority and/or precedence, or assurance (signature and/or encryption) as organizational messages. Individual messaging is accomplished using office automation (e.g., Simple Mail Transfer Protocol electronic mail) via the inter- or intra network (e.g., SECRET Internet Protocol Router Network (SIPRNET)). DMS is not intended for individual messaging.

6. Responsibilities

a. Each combatant command will develop and implement DMS procedures that include roles, responsibilities, and related implementation issues. These plans will identify pertinent message-processing support to the component

commands, non-DOD U.S. agencies, and allied and/or coalition supporters, as necessary, to meet operational requirements. Shortfalls in messaging interoperability must be addressed with their executive agents and/or component commands.

b. J-3 will develop policy and guidance for products, architectures, configuration, and capabilities that handle OPLAN 8010 (reference d) information.

c. The host Military Department or agency will provide Internet protocol router and application layer message handling services (e.g., DMS) to tenants on base, post, camp, or station. Local host and/or tenant agreements or inter-Service support agreements may include cost recovery where appropriate.

7. Summary of Changes

a. Updated definition of organizational message.

b. Updated references and acronyms.

c. Corrected minor grammatical errors.

8. 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 CJCS Directives Home Page—http://www.dtic.mil/cjcs_directives—on the Internet.

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

WILLIAM E. GORTNEY
VADM, USN
Director, Joint Staff

Enclosure(s):

A – Defense Message System Policy

B – Defense Message System Documentation Hierarchy

C – References

GL – Glossary

(INTENTIONALLY BLANK)

DISTRIBUTION

Distribution A, B, C, and JS-LAN plus the following:

	Copies
Commander, U.S. Element North American Aerospace Defense Command (NORAD)	2
Commander, Joint Interoperability Test Command (JITC)	2
Chairman, Inter-American Defense Board	2
United States National Military Representative (USNMR) to Supreme Headquarters Allied Powers, Europe (SHAPE)	2
United States Representative to the Military Committee (USRMC) (NATO) Liaison Office	2
United States Liaison Officer (USLO) to Supreme Allied Commander, Transformation (SACT)	2
Office of Director of National Intelligence/Chief Information Officer (ODNI/CIO)	2

(INTENTIONALLY BLANK)

TABLE OF CONTENTS

(INTENTIONALLY BLANK)

ENCLOSURE A

DEFENSE MESSAGE SYSTEM POLICY

1. Defense Message System Description

a. DMS is the DOD system of record for all organizational message traffic. It employs an X.400 open systems interconnection protocol standard and the X.500 networking standards for directory services and security services based on the multi-level information system security initiative (MISSI) protocol guidelines. For transmission paths between its components, DMS relies primarily on the Defense Information System Network (reference e) Transmission Control Protocol/Internet Protocol (TCP/IP) networks: the Non-Secure Internet Protocol Router Network (NIPRNET) and the SIPRNET; local area networks; and other wide area networks, such as the Joint Worldwide Intelligence Communication System (JWICS) and other sensitive compartmented information (SCI) networks. DMS supports organizational messaging at the unclassified, SECRET, and TOP SECRET collateral levels.

b. DMS consists of all hardware, software, policy, procedures, standards, facilities, and personnel used to exchange organizational messages electronically between DOD organizations and other U.S. and non-U.S. governmental organizations.

c. The DMS architecture provides a framework for a Service and/or agency implementation and a managed backbone infrastructure. The architecture does not limit an organization to a design in terms of a "site," referring to a specific geographic location. The DMS architecture is extensible and supports a multi-location groupware design to take maximum advantage of the capability in today's collaborative computing products. Local implementations will vary depending on the implementing architecture/products (e.g., large/medium/small, tactical/fixed, classified/unclassified, etc.) and local support, business practices, and interfaces. Users should familiarize themselves with local standard operating procedures for specific DMS implementation methods.

2. U.S. Message Text Format. The Military Services, combatant commands, Joint Staff, combat service support commands, and those other activities and agencies responsive to the Chairman of the Joint Chiefs of Staff will use USMTF for all organizational messaging (reference f). A USMTF editor used in conjunction with DMS provides a secure communications and information process that can accommodate the

widest range of missions and operational environment. The use of attachments with DMS messages prepared using USMTF is authorized.

3. DOD Organizational Messaging Infrastructure

a. DMS

(1) DMS is structured to provide an interoperable, seamless, and secure electronic messaging system for organizational users within the Department of Defense. DMS uses commercial-based products for drafting, coordinating, and releasing messages. DMS is the DOD system of record for all organizational message traffic (reference g).

(2) DMS components are based on the internationally developed ITU-T-X.400 message handling and X.500 directory service systems. MISSI security mechanisms and common security protocol (CSP), developed by the National Security Agency (NSA) provide DMS security services to ensure the protection of DOD unclassified and classified information.

(3) The DMS implementation architecture is accomplished via a domain environment. The original DMS architecture was client-server. This was cumbersome to the end-users, each of whom had to carry and maintain a FORTEZZA (PKI) card. The DMS domain-to-domain architecture is often called domain FORTEZZA because it moves the FORTEZZA-based security processing from the user's workstation to a server. The users (message releasers and recipients) access these servers via Web or e-mail clients on their workstations, authenticate themselves to the servers, and send/receive messages via these services. Based upon the user's authenticated identity, the server determines the user's authorizations for sending/receiving messages. The server performs FORTEZZA-based security processing and X.400 message transfers.

b. Nuclear Command, Control, and Communications (NC3) Hybrid Solution (HS)

(1) The NC3 HS Emergency Action Message (EAM) architecture supports fixed and mobile EAM injectors and recipients and provides for EAM dissemination to time critical (TC) and non-TC users. TC users include those users who are required to receive messages within the time constraints imposed by the nuclear technical performance criteria and other users determined to be TC by the Joint Staff. In addition to EAM dissemination, the NC3 HS provides transport for the general service (GENSER) traffic up to TOP SECRET OPLAN 8010 (reference h) and Nuclear Planning and Execution System (NPES) traffic to and from the

Survivable Mobile Command Center community, and those fixed command center sites that employ NPES.

(2) EAMs are highly structured, authenticated messages primarily used in the C2 of nuclear forces. EAMs are disseminated over numerous survivable and non-survivable communication systems, including terrestrial and space systems. The NC3 HS is the principal means of dissemination of EAMs in a pre-attack environment. The NC3 HS comprises several existing systems including the Navy's Nova, the Air Force's Strategic Automated Command Control System, the Defense Improved Emergency Message Automatic Transmission System Replacement Command and Control Terminal, the DMS, and the Pentagon Telecommunications Center. The primary interface between the NC3 HS and DMS are the National Gateway Centers.

c. National Gateway Centers

(1) The NGCs provide a standard interface to other government agencies, allies, defense contractors, and other approved activities external to the DMS community. The NGCs provide messaging interoperability with allies, coalition partners, and non-DOD U.S. agencies (e.g. Department of State, Department of Justice). This interoperability is secure, reliable, and survivable. The NGCs provide messaging interoperability at all levels of classification and access as required by the user.

(2) The NGCs are located at: the Pentagon, Washington, D.C., and Fort Detrick, Maryland. Defense Information Systems Agency (DISA) manages the NGCs in coordination with the U.S. Army. The Service provides switching between legacy message (ACP 128 U.S. SUPP-1 dated Nov 05) users as well as translations between legacy organizational and DMS users in both directions.

4. Authorities

a. Joint Staff, Directorate of Operations. The Joint Staff/J-3 is the approving authority for declaring EAM messaging systems acceptable and the system of record for EAM dissemination. Additional EAM roles and responsibilities for the combatant commands, Services, agencies (C/S/A) are outlined in reference i.

b. C/S/A. C/S/A will field, operate, and maintain DMS components and associated message processing systems within their domains. C/S/A must also obtain the necessary approval for employment of DMS components and products being connected to the local enterprise network transport layers (NIPRNET, SIPRNET, JWICS, etc.).

c. DISA. DISA is the lead agency for the DMS program. The Director, DISA, exercises program management oversight in accordance with DODD 5000.2-R (reference j). This oversight consists of adhering to the requirements for a joint program, to include system design, engineering, acquisition, implementation, integration, operational direction, and management control over all elements of DMS as a Global Information Grid component, per reference k. Additionally, DISA designs, develops, tests, and maintains all DMS infrastructure (backbone) products. DISA responsibilities include, but are not limited to, life-cycle support and management, configuration control, and technical refresh of components and products.

d. Joint Interoperability Test Command (JITC). The Commander, JITC, administers developmental testing, integration testing, and operational testing of DMS components, per reference k.

5. Security. Security approvals, in accordance with the DOD Information Assurance Certification and Accreditation Process (DIACAP) (reference l), are the joint responsibility of the NIPRNET, SIPRNET, and DOD SCI networks designated approving authorities (DAA). Per DMS security policy (reference ddd) and DMS Trusted Facility Manual (reference m), security protection is required for all messaging products at all classification levels. NSA-approved security protection mechanisms protect DMS messages. The DAAs determine the overall adequacy of security protection. The DMS products, architectures, configurations, and capabilities must adhere to Director, Central Intelligence Directive (DCID), 6/3 (reference n) security standards before operation of DMS within SCI security domains.

a. The NSA will approve products, architectures, configurations, and capabilities that handle and support critical communications information. Additionally, NSA will exercise life cycle support to include program management, system design, and acquisition over information assurance elements of the DMS program per reference o.

b. The Defense and Intelligence Community Accreditation Support Team (DICAST) reviews and advises for the Intelligence Community (IC) CIO on systems with three or more principal accrediting authorities. This team will review the SCI DMS components for community inclusion for operation across the IC DOD.

c. DISA will approve products, architectures, configurations, and capabilities that handle GENSER information, not including OPLAN 8010 (reference d). Each C/S/A operating DMS GENSER will accredit that product and/or system implementation in accordance with local

procedures, based upon DISA's and/or NSA's type accreditation for that product and/or system implementation. DISA will ensure that all DIACAP requirements for type accreditation are met (reference l).

d. Joint Staff/J-3 will approve products, architectures, configurations, and capabilities that handle OPLAN 8010 (reference d) information. The Joint Staff and C/S/As are responsible authorities for determining users with a need to process OPLAN 8010 messages (reference d). The Director, Joint Staff, is the DAA for all OPLAN 8010 accreditation. Joint Staff/J-3 is the executive agent for all Joint Staff OPLAN 8010 DAA actions.

6. Approval Procedures for DMS Services for Non-DOD Activities

a. U.S. government non-DOD organizations may be considered for DMS services, upon OSD approval, if any of the following conditions exist:

(1) The requirement is considered necessary for C2 and cannot be satisfied by other means.

(2) The requirement supports a DOD mission.

(3) They are sponsored by a DOD activity.

(4) Other justification OSD deems appropriate.

b. U.S. non-government organizations 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 OSD deems appropriate.

c. Non-U.S. activities may be considered for DMS services. Requests are processed under the provisions of reference a. As appropriate, OSD will direct DISA to effect or facilitate implementation.

(INTENTIONALLY BLANK)

ENCLOSURE B

DEFENSE MESSAGE SYSTEMS DOCUMENTATION HIERARCHY

1. Overview

a. DMS program governance is provided in DOD regulation, Allied Communications Publications (ACP), CJCSIs and CJCSMs, DISA circulars and interim procedures, Service/agency procedures, and local operating procedures. The order of precedence for these various documents is as follows:

(1) U.S. Department of Defense

(2) Allied Communication Publications

(3) Chairman of the Joint Chiefs of Staff (CJCS) publications

(4) DISA circulars

(5) DISA interim procedures

(6) Service/agency publications

(7) Local operating instructions

b. Conflicts between document(s) will be resolved using the above precedence.

2. Department of Defense Publications

a. DODD 5100.55, "U.S. Security Authority for North Atlantic Treaty Organization Affairs, United States Security Authority for NATO (USSAN) Instruction 1-69, North Atlantic Treaty Organization (NATO) Security Program." Updates policies and procedures for the United States Security Authority for NATO Affairs. Outlines methods to be used in transmitting NATO policies and procedures within the Department of Defense and assigns responsibilities for maintaining NATO security worldwide. This directive is applicable to OSD, Services, Joint Chiefs of Staff, and the combatant commands (reference p).

b. DODD 5200.1-R, "DOD Information Security Program." Updates polices and procedures for information security within the Department of Defense. Provides definitions for compromise, information, and national security. This directive applies to OSD, Military Services, Joint Chiefs of Staff,

combatant commands, Inspector General of the Department of Defense, Defense agencies, and the DOD field activities (reference q).

c. DODD 5200.2-R, "Personnel Security Program." Updates policies and responsibilities for the Department of Defense Personnel Security Program. The purpose of the program is to ensure the military, civilian, and contractor personnel working in sensitive positions are reliable and trustworthy. This directive applies to OSD, Services (including the Coast Guard when it is operating as a Military Service under the Navy), Joint Chiefs of Staff, combatant commands, Inspector General of the Department of Defense, Defense agencies, and the DOD field activities. Additionally, this directive applies to DOD civilian personnel, members of the Armed Forces (including the Coast Guard when it is operating under the Department of Defense as a Service in the Department of the Navy), contractor personnel and other personnel affiliated with the Department of Defense (reference r).

d. DODI 8510.01, DOD Information Assurance Certification and Accreditation Process, 28 November 2007. Establishes the DOD information assurance (IA) certification and accreditation process for authorizing the operation of DOD information systems consistent with the Federal Information Security Management Action (FISMA), DODD 8500.1, and DOD 8100.1. This instruction provides visibility and control of the implementation of IA capabilities and services, the C&A process, and accreditation decisions authorizing the operation of DOD information systems, to include core enterprise services and Web services-enabled software systems and applications (reference l).

3. Allied Communication Publications

a. ACP 117 (N), "Allied Routing Indicator Book." This publication provides information for the routing of message traffic within and/or between communications systems and for the transfer of message traffic between national communications systems. This ACP contains a list of the routing indicators and routing information to be used on the common-user data networks of the United States and selected allies. There are several supplements to ACP 117, for example CAN-U.S. Supp-1, NATO Supp-1, and others. All U.S. plain language addresses that appear in ACP 117 NATO Supp-1 must have organizational accounts that can accept NATO messages. The organizational accounts must have the correct certificates to allow the receipt of legitimate NATO classified messages. A companion document to ACP 117 is ACP 121, "Routing Indicator Delineation Table." (reference s)

b. ACP 120, "Common Security Protocol (CSP)." Describes the services and protocols implemented in a common security protocol user agent for secure electronic mail and security messaging. The CSP user agent is used

with the Consultative Committee for International Telegraphy and Telephony X.400 Message Handling System (reference t).

c. ACP 127, "Communications Instructions – Tape Relay Procedures." This publication prescribes the procedure to be employed for the handling of messages by manual, semiautomatic or fully automatic relay systems, referred to collectively as Tape Relay (reference u).

d. ACP 128, "DOD Information Assurance Certification and Accreditation Process. "This publication prescribes the operating procedures and practices applicable to the Allied Telecommunications Record System (ALTERS) and to other record communications networks as specifically authorized by respective controlling authorities (reference v).

e. ACP 133(D), "Common Directory Services and Procedures." This ACP defines the directory services, architecture, protocols, schema, policies, and procedures to support allied communications, including Military Message Handling System services based on ACP 123, in the strategic and tactical environments (reference w).

f. ACP 145(A), "Interim Implementation Guide for ACP 123/STANAG 4406 Messaging Services Between Nations." ACP 123/STANAG 4406, ACP 133, and this ACP define the standards for messaging, security, and directory services required to achieve military messaging based on X.400 technology. Due to differences in national implementations of messaging services and the complexity of achieving full end-to-end security services between nations, messaging between these nations will be by way of gateway services with security services provided using secure Multipurpose Internet Mail Extensions (MIME), version 3, with its enhanced security services (reference x).

4. Chairman of the Joint Chiefs of Staff

a. CJCSI 6241.04, "Policy and Procedures for Using United States Message Text Formatting." This instruction implements policy and procedures for management and use of USMTF in DOD information technology systems. The use of common warfighting syntax and content standards provides the foundation for seamless communications and the decisive factor that enables sound decision making and information superiority. Use of USMTF is mandatory in conjunction with DMS (reference f).

b. CJCSM 6231.01D, "Manual for Employing Joint Tactical Communications." This manual serves as the umbrella document that sets the framework and guidance for developing tactics, techniques, and procedures (TTPs) necessary to support integration of communications networks and Internet Protocol (IP) based net-centric capabilities required to support a Joint Task Force, Joint Special Operations Task Force, or other military operations.

It identifies the communications concepts, provides guidance for planning and employing joint tactical communications equipment and serves as guidance for lesson plan development associated with the Joint C4 Planners Course (JC4PC). It also provides the procedures to develop and maintain technical standards, TTPs, and procedures for joint tactical communications and shifts the overall management and update process to an online collaboration Web site. (reference y)

c. CJCSM 6231.04, "Manual for Employing Joint Tactical Communications, Joint Transmission Systems." This manual provides information and guidance on planning, engineering, installing, and managing transmission systems that support joint exercises and contingency operations. Cancelled as of 15 Jan 10 (reference z).

d. CJCSI 6740.01B, "Military Telecommunications Agreements and Arrangements between the United States and Regional Defense Organizations or Friendly Foreign Nations." This instruction provides policy on negotiating and concluding international military telecommunication agreements and arrangements to sell or exchange telecommunications support or services to allow the transfer of data and voice traffic between the United States and regional defense organizations or friendly foreign nations (reference a).

5. Defense Information Systems Agency Publications

a. Circulars

(1) DISA Circular 310-D70-30, "Global Information Grid (GIG) National Gateway Center (NGC) and Subscriber Operations." Circular assigns responsibilities and provides procedures for the operation of legacy message switching portion of the GIG NGC (formerly the Automatic Digital Network (AUTODIN) Switching Center [ASC] and Defense Message System [DMS] Transition Hub [DTH] and for subscriber use of the NGC legacy messaging network. The GIG NGCs comprise legacy messaging switches at Ft. Dietrick and the Pentagon Telecommunications Center (PTC) to include the PTC backup switch at Site-R (reference aa).

(2) DISA Circular 310-130-2, "Management Thresholds and Performance Objectives." Circular prescribes the performance measurement standards in terms of management thresholds and performance objectives that DISA will use for the telecommunications portion of the Global Information Grid (GIG). (reference bb).

b. Interim Procedures

(1) Interim Procedure 01, "Defense Message System, DMS Operations Coordination Messages and Interim Procedures." This procedure identifies the method of communication between the DMS operational staff elements of the

global service manager (GSM), regional service manager, area system manager, local system manager, and the NGCs. It establishes and defines interim procedures and their applicability. The ALDMSSTA address list is contained in this procedure (reference cc).

(2) Interim Procedure 02, "Defense Message System Message Trace Procedures." Provides policy and procedures for requesting and coordinating DMS message tracing between the DMS area control centers and local control centers (ACC/LCC), DMS network operation centers (DMS-NOC), and between the NGCs and the DMS NOC. The purpose of a message trace is to determine the cause of non-delivery or corruption of a DMS organizational message to an intended recipient. This procedure established the message delivery threshold and the tracer processing timeframes (reference dd).

(3) Interim Procedure 03, "Defense Message System, Configuration Change Procedures." Outlines the procedures for implementing DMS configuration changes at commissioned DMS ACC, LCC, and sites. Updates the ACC/LCC/site detailed designs and master system detailed design. Defines procedures for coordinating DMS backbone changes with the DMS NOC (reference ee).

(4) Interim Procedure 04, "Defense Message System, System Upgrade Procedures." Provides the operational transition procedures for upgrading the global DMS system, infrastructure and ACC/LCC enclaves with new product releases (commercial and government). Defines emergency field engineering notice (FEN) procedures, weekend and holiday emergency FEN procedures, non-duty hour FEN process implementation, and points of contact (reference ff).

(5) Interim Procedure 05, "Defense Message System, Field Engineering Notice (FEN) and Advisory Note (AN) Distribution and Installation Procedures." Provides policy, procedures, and guidance for the distribution, documentation, and implementation of the FEN and AN for the DMS. Outlines GSM responsibility for the approval, usage, authorization, and dissemination of software for use on the DMS. System operation managers will only allow the installation of GSM-authorized FEN and software patches (reference gg).

(6) Interim Procedure 06, "Defense Message System, DMS Problem Management." Describes the roles, responsibilities, policy, procedures, and standards for the coordination of problem management in the DISA Trouble Management System for the DMS environment between the various combatant commanders, Military Services, and/or agency help desks, area control centers, local control centers, the NGCs, the DISA DMS NOCs, and the DMS integration contractor (reference hh).

(7) Interim Procedure 07, "Defense Message System, DMS Ports, Protocols, and Service (PPS) Reference Guide." Identifies DMS use of ports,

protocols, and services. Assists firewall and router administrators in the configuration of Service and agency implemented firewalls and routers to support DMS operations. Illustrates logical connectivity requirements and provides DMS ports, protocols, and services information for a representative local firewall implementation (reference ii).

(8) Interim Procedure 08, "Defense Message System, DMS Asset Distribution System (DADS) Registration for Site Commissioning." Identifies the requirement for new DMS ACC and LCC to register on the DADS prior to site commissioning testing with the Regional Operations and Security Center. The DADS is a secure socket site that uses encryption to protect transmitted information. Users must have a signed certificate associated with their Internet browser to access DADS (reference jj).

(9) Interim Procedure 09, "Defense Message System, Procedures and Guidelines for Establishing DMS Organizational Users." Describes the process for DMS organizational users to be provided with a distinguished name in the global directory, establishing a unique personality and associated security information, as well as an originator and/or recipient address. Additionally, provides a discussion on the various options that a DMS organization may select. Each organization can design its messaging plan to meet the requirements of the organization with the DMS flexible architecture (reference kk).

(10) Interim Procedure 10, "Defense Message System, Test Site Roles and Responsibilities." Reviews the operational policies and procedures relating to the testing of software and/or hardware products on the operational DMS and within off-line test site environments. Describes the roles and responsibilities of Service and/or agency sites implementing products for test purposes under the direction of the DMS GSM (reference ll).

(11) Interim Procedure 11, "Defense Message System, Authorized Service Interruptions." Rescinded 30 May 2006 (reference mm).

(12) Interim Procedure 12, "Defense Message System, Outage Reporting and System Status Notification Procedures." Identifies the criteria and procedures for DMS outage reporting to the DMS NOC, Global Network Operations (NetOps) and Support Center, and the DMS GSM for system monitoring and management purposes. Also outlines procedures for dissemination of this information to the Military Services, agencies, area and local control centers, NOC, and NGCs for system status awareness (reference nn).

(13) Interim Procedure 13, "Defense Message System, Enhancement Recommendation Process Procedures." Outlines the policy and procedures for processing recommended DMS enhancements. DMS product enhancements are modifications and additions to DMS products (e.g., software, hardware), which are not intended to correct a product defect. This procedure is designed

for handling the recommended system enhancements, ensuring full review and coordination prior to final decision, and commitment of resources (reference oo).

(14) Interim Procedure 14, "Defense Message System, High Assurance Guard (HAG) Acceptance and Commissioning Procedures. Rescinded 15 Oct 2008 (reference pp).

(15) Interim Procedure 15, "Defense Message System, DMS Information Assurance Vulnerability Alert (IAVA) Process Roles and Responsibilities." Describes the DISA DMS IAVA process and the roles and responsibilities associated with this process. The DISA DMS GSM is the DMS IAVA program manager for the DOD IAVA process. The DMS IAVA program manager provides guidance through the DMS IAVA process to the community for handling vulnerability notifications, including implementation of GSM-authorized corrective actions. The DMS IAVA process does not generate vulnerability notifications (reference qq).

(16) Interim Procedure 16, "Defense Message System, Defense Message System (DMS) Asset Distribution System (DADS) Registration Process." Outlines the registration process and procedures to be followed when requesting access to the DADS. Provides a discussion on the roles and responsibilities associated with the registration process (reference rr).

(17) Interim Procedure 17, "Defense Message System, DMS Deployed Procedures." Defines policy, procedures, and criteria for commissioning deployed and/or tactical DMS components into the DMS global network. Focuses on the procedures and criteria used to verify the operational readiness of the tactical DMS infrastructure to interface with the strategic DMS infrastructure. Tactical gateway components that deployed units install are commissioned to ensure the installation is in accordance with approved implementation plans and detailed system designs and are capable of performing their intended functions (reference ss).

(18) Interim Procedure 18, "Defense Message System, DoD Address List Procedures." Outlines the policies and procedures for requesting, managing, maintaining, and using DOD-level address lists. Identifies the Address List Management Center located at the NGC, Fort Detrick, Maryland, as the DOD-level address lists administrator (reference tt).

(19) Interim Procedure 19, "Defense Message System, Service and Agency Address List Procedures." Defines the procedures implemented by the Services and/or agencies with regard to address list management. Defines roles and responsibilities with regard to address list management and maintenance and specifies the information that is to be populated in address list directory entries as well as supporting directory entries of management personnel. Additionally, identifies the multi-functional interpreters that need to be included as authorized submitters to address lists and presents common

handling procedures for non-delivery notices resulting from messages addressed to address lists (reference uu).

(20) Interim Procedure 20, "Defense Message System, Field Engineer Notice (FEN) Acceptance and Release Process: Roles and Responsibilities." Describes the DMS FEN acceptance and release process. Defines the roles and responsibilities of the organizations involved in this process. The document discusses the process from the pre-compliant FEN submission to the DISA DMS GSM, through testing, approval, and dissemination of the GSM-authorized DMS compliant product (reference vv).

(21) Interim Procedure 21, "Defense Message System, Security Spillage Procedures." Identifies the procedures to be followed in the event of a security spillage at any of the DISA-controlled DMS sites. For the purposes of this procedure, a security spillage is defined as a situation where a DMS component has received, stored, and/or processed a message that is classified at a category higher than the DMS component should allow. Additionally, this procedure defines the four DMS security environments as the NIPRNET, SIPRNET, virtual private network over the SIPRNET for TOP SECRET-Collateral, and the IC. This procedure does not address a spillage in the IC environment (reference ww).

(22) Interim Procedure 22, "Defense Message System, External Field Engineer Notice (FEN) and External Advisory Note (AN) Procedures." Describes policy and procedures for the development of FEN documentation, software patches, procedures, or advisory notes by organizations external to the DMS prime contractor. This interim procedure supplements interim procedure 05 (reference xx).

(23) Interim Procedure 23, "Defense Message System, Directory Performance Monitoring." Outlines policy and procedures for the collection and forwarding of directory service agents (DSAs) log data for use by DISA. DISA will use the data to analyze the performance of all global DSAs and selected local directory service agents. The root global and the plain language DSAs are not normally evaluated (reference yy).

(24) Interim Procedure 24, "Defense Message System, Policies and Procedures for Software Distribution." Outlines the policies and procedures used when distributing DMS software and maintenance releases with associated field engineering notices and advisory notes (reference zz).

(25) Interim Procedure 25, "Defense Message System, Integrated Architectural Database (DIAD) Registration Process." Identifies the registration process and procedures for the DMS Integrated Architectural Database (DIAD) and the roles and responsibilities associated with this process. The DIAD provides an electronic population, storage, dissemination, management, and control of information describing the network detailed designs of the DMS

strategic and deployed sites communicating on the NIPRNET and SIPRNET (reference aaa).

(26) Interim Procedure 26, "Defense Message System, Nuclear Command, Control, and Communications (NC3) Global Hybrid Network Messaging Service Management." Discusses the network connectivity being used to support the dissemination of NC3 messages. The networks supporting NC3 messaging consist of the Navy's Nova, Air Force's Strategic Automated Command and Control System, Air Force's Cheyenne Mountain and Offutt Communications Support Processors, and the Fort Detrick NGC (reference bbb).

(27) Interim Procedure 27, "Defense Message System, Directory Security." Discusses the policies and procedures for DMS directory security. These policies and procedures consolidate IC directory requirements with the general service requirements. Provides a brief discussion on organizational roles and responsibilities (reference ccc).

(28) Interim Procedure 28, "Defense Message System, Configuration Management Terminology Abbreviations and Acronyms." Provides a reference for DMS terminology and abbreviations used in DMS configuration management documentation (reference ddd).

(29) Interim Procedure 29, "Defense Message System, Defense Message System Asset Distribution System User Guide." The purpose of this interim procedure is to provide a quick reference to assist DADS users in managing their passwords and account information, finding and selecting FEN, and providing assistance in navigating the DADS (reference eee).

(30) Interim Procedure 30, "Defense Message System, Defense Message System Security." Provides DMS security guidance for computer systems running DMS applications and systems interfacing with DMS by consolidating current DMS security procedures, policies, and advisories. Provides overview of the roles and responsibilities of the organizations tasked with meeting the DMS directory security requirements (reference fff).

(31) Interim Procedure 31, "Defense Message Systems, DMS Policy and Procedures for the Multi-Function Interpreter (MFI) and MFI-Like Devices Validation Process." Prescribes the policies, procedures, and criteria for validation and approval to operate the MFI and MFI-like devices in the DMS. The term MFI represents DMS core MFI and Configuration Management Board-approved non-core MFI-like products (e.g., secure messaging and routing terminal and/or communications support processor to DMS addressing component). Outlines the responsibilities for verifying that MFI devices have been installed and configured using appropriately certified components in accordance with prescribed operational, technical, and security directives (reference ggg).

(32) Interim Procedure 32, "Defense Message System, DMS Acceptance and Commissioning of DMS Sites and Infrastructure Components." Defines policy, procedures, and criteria for acceptance and commissioning of DMS sites and/or infrastructure components directly connected to the DMS global backbone. Outlines roles and responsibilities in support of the installation test, acceptance, and commissioning process that must be performed in order to accomplish the acceptance and commissioning of DMS infrastructure sites and components (reference hhh).

(33) Interim Procedure 33, "Defense Message System, DMS Version 3 X.509 GENSER End User Certificate Request Forms Package." Provides instructions to complete the X.509 end-user request forms package to obtain a class 4 certificate and FORTEZZA card. This interim procedure will be used for requesting the class 4 certificate in a client and/or server or DMS domain environment. This interim procedure applies only to X.509 certificate and FORTEZZA requests for GENSER DMS (reference iii).

(34) Interim Procedure 34, "Defense Message System, Proxy User Agent Policy Implementation Instruction." Provides detailed instructions regarding security mechanisms required for implementation of DMS proxy user agent (PUA) systems (also referred to as domain FORTEZZA systems) in a manner that adequately protects the DMS from unauthorized message origination or reception, as well as providing a high degree of protection of the integrity of DMS messages sent/received by DMS PUA systems (reference jjj).

(35) Interim Procedure 35, "Defense Message System, Defense Information Systems Agency-Combined Communications Electronics Board Public Key Infrastructure Issuance Procedure v 1.0." Provides guidance on how DISA will process unclassified DOD PKI certificate requests on a classified network from a foreign Combined Communications Electronics Board (CCEB) government and physically issue the server certificates (reference kkk).

(36) Interim Procedure 36, "Defense Message System, Policies and Procedures for the National Gateway Centers (NGCs) and the Navy Tactical Messaging Gateways (TMGs)." Provides standardized policies and procedures for the NGCs and the Navy TMGs. The IP is designed to ensure the legacy and DMS user community issues are resolved in the same manner by all NGCs and TMGs. In addition, this document contains the contingency MFI FORTEZZA card process and the required reporting procedures (reference lll).

ENCLOSURE C

REFERENCES

a. CJCSI 6740.01 series, "Military Telecommunications Agreements and Arrangements Between the United States and Regional Defense Organizations or Friendly Foreign Nations"

b. National Disclosure Policy Directive (NDP-1) (U), 2 October 2000

c. CJCSI 5221.01 series, "Delegation of Authority to Commanders of combatant commands to Disclose Classified Military Information to Foreign Governments and International Organizations"

d. CDRUSSTRATCOM OPLAN 8010-08, Global Deterrence and Strike, 1 December 2008 (S/FRD/NF)

e. CJCSI 6211.02 series, "Defense Information System Network (DISN): Policy, Responsibilities and Procedures"

f. CJCSI 6241.04 series, "Policies and Procedures for Using United States Message Text Formatting"

g. ASD (C3I) memorandum, 12 April 2001, "Update to the Revised Defense Message System Transition Plan"

h. CJCSI 3231.01 series, "Safeguarding Nuclear Command and Control Extremely Sensitive Information"

i. Joint Staff, 5 October 2001, "Emergency Action Message Hybrid Solution Management Plan"

j. DODD 5000.2-R, 5 April 2002, "Mandatory Procedures for Major Defense Acquisition Program (MDAPs) and Major Automated Information Systems (MAIS) Acquisition Programs"

k. DODD 5105.19, 25 July 2006, "Defense Information Systems Agency (DISA)"

l. DODI 8510.01, 28 November 2007, "DOD Information Assurance Certification and Accreditation Process"

m. DISA manual, 1 October 2001, "DMS Trusted Facility Manual"

n. Director, Central Intelligence, Directive (DCID) 6/3, 5 June 1999, "Protecting Sensitive Compartmented Information within Information Systems"

o. DCID 1/7, 30 June 1998, "Security Controls on the Dissemination of Intelligence Information"

p. DODD 5100.55, 27 February 2006, "U.S. Security Authority for North Atlantic Treaty Organization Affairs, United States Security Authority for NATO (USSAN) Instruction 1-69, North Atlantic Treaty Organization (NATO) Security Program"

q. DODD 5200.1-R, 14 January 1997, "DOD Information Security Program"

r. DODD 5200.2-R, 9 April 1999, "Personnel Security Program"

s. Allied Communications Publication 117(N), September 2006, "Allied Routing Indicator Book"

t. Allied Communications Publication 120, June 1998, "Common Security Protocol"

u. Allied Communications Publication 127, November 1988, "Communications Instructions – Tape Relay Procedures"

v. Allied Communications Publication 128, December 1996, "Allied Telecommunications Record System Operating Procedures"

w. Allied Communications Publication 133(D), July 2009, "Common Directory Services and Procedures"

x. Allied Communications Publication 145(A), September 2008, "Interim Implementation Guide for ACP 123/STANAG 4406 Messaging Services Between Nations"

y. CJCSM 6231.01D, 15 January 2010, "Manual for Employing Joint Tactical Communications"

z. CJCSM 6231.04, "Manual for Employing Joint Tactical Communications, Joint Transmission Systems" (Canceled as of 15 January 2010)

aa. DISA Circular 310-D70-30, 21 November 2005, "Global Information Grid (GIG) National Gateway Center (NGC) and Subscriber Operations"

bb. DISA Circular 310-130-2, 14 November 2005, "Management Thresholds and Performance Objectives"

cc. Interim Procedure 01, 2 October 2008, "Defense Message System, DMS Operations Coordination Messages and Interim Procedures"

dd. Interim Procedure 02, 2 October 2008, "Defense Message System Trace Procedures"

ee. Interim Procedure 03, 9 March 2010, "Defense Message System, Configuration Change Procedures"

ff. Interim Procedure 04, 8 October 2008, "Defense Message System, System Upgrade Procedures"

gg. Interim Procedure 05, 28 October 2006 Defense Message System, Field Engineering Notice and Advisory Note Distribution and Installation Procedures

hh. Interim Procedure 06, 18 February 2009 Defense Message System, DMS Problem Management

ii. Interim Procedure 07, 16 August 2006, "Defense Message System, DMS Ports, Protocols and Service Reference Guide"

jj. Interim Procedure 08, 10 March 2010, "Defense Message System, DMS Asset Distribution System Registration for Site Commissioning"

kk. Interim Procedure 09, 28 March 2008, "Defense Message System, Procedures and Guidelines for Establishing DMS Organizational Users

ll. Interim Procedure 10, 28 September 2006, "Defense Message System, Test Site Roles and Responsibilities"

mm. Interim Procedure 11, 3 May 06, "Defense Message System, Authorized Service Interruptions" (Rescinded 30 May 2006)

nn. Interim Procedure 12, 18 February 2009, "Defense Message System, Outage Reporting and System Status Notification Procedures"

oo. Interim Procedure 13, 22 October 2009, "Defense Message System, Enhancement Recommendation Process Procedures"

pp. Interim Procedure 14, 15 October 2008, "Defense Message System, High Assurance Guard Acceptance and Commissioning Procedures (Rescinded 15 October 2008)

qq. Interim Procedure 15, 19 July 2007, "Defense Message System, DMS Information Assurance Vulnerability Alert Process Roles and Responsibilities"

rr. Interim Procedure 16, 1 October 2009, "Defense Message System, Defense Message System Asset Distribution System Registration Process"

ss. Interim Procedure 17, 31 October 2008, "Defense Message System, DMS Deployed Procedures

tt. Interim Procedure 18, 5 October 2009, "Defense Message System, DoD Address List Procedures

uu. Interim Procedure 19, 9 December 2008, "Defense Message System, Service and Agency Address List Procedures"

vv. Interim Procedure 20, 20 September 07, "Defense Message System, Field Engineering Notice Acceptance and Release Process: Roles and Responsibilities"

ww. Interim Procedure 21, 11 June 2008, "Defense Message System, Security Spillage Procedures"

xx. Interim Procedure 22, 24 September 2007, "Defense Message System, External Field Engineer Notice (FEN) and External Advisory Note (AN) Procedure"

yy. Interim Procedure 23, 24 September 2007, "Defense Message System, Directory Performance Monitoring

zz. Interim Procedure 24, 24 September 2007, "Defense Message System, Policies and Procedures for Software Distribution"

aaa. Interim Procedure 25, 8 October 2009, "Defense Message System, Integrated Architectural Database Registration Process"

bbb.. Interim Procedure 26, 28 June 2005, "Defense Message System, Nuclear Command, Control, and Communications Global Hybrid Network Messaging Service Management"

ccc. Interim Procedure 27, 21 July 2003, "Defense Message System, Directory Security"

ddd. Interim Procedure 28, 29 October 2008, "Defense Message System, Configuration Management Terminology Abbreviations and Acronyms"

eee. Interim Procedure 29, 14 April 2006, "Defense Message System, Defense Message System Asset Distribution System User Guide"

fff. Interim Procedure 30, 24 September 2009, "Defense Message System, Defense Message System Security"

ggg. Interim Procedure 31, 31 June 05, "Defense Message System, DMS Policy and Procedures for the Multi-Function Interpreter (MFI) and MFI-Like Devices Validation Process"

hhh. Interim Procedure 32, 14 June 2009, "Defense Message System, DMS Acceptance and Commissioning of DMS Sites and Infrastructure Components"

iii. Interim Procedure 33, 28 October 2008, "Defense Message System, DMS Version 3 X.509 GENSER End User Certificate Request Forms Package"

jjj. Interim Procedure 34, 27 November 2009, "Defense Message System, Proxy User Agent Policy Implementation Instruction"

kkk. Interim Procedure 35, 2 February 2006, "Defense Message System, Defense Information System Agency-Combined Communications Electronics Board Public Key Infrastructure Issuance Procedure v 1.0"

lll Interim Procedure 36, 15 May 07, "Defense Message System, Policies and Procedures for the National Gateway Centers (NGCs) and the Navy Tactical Messaging Gateways (TMGs)"

OTHER RELEVANT PUBLICATIONS

DOD/CIO memorandum, 6 January 2010, "Strategy for Defense Message System Migration to Official Information (OI) and Organizational Messaging (OM) Service Oriented Enterprise Solutions"

The following DISA circulars are being drafted for signatures. The policies and procedures contained within are widely known within the DMS user community.

DISA Circular 310-M70-87, "Methods and Procedures Operational Policies and Procedures for the Defense Message System." This circular defines policy, identifies or assigns responsibilities, and provides procedures for the operational direction and management control of the DMS. The circular is applicable to the DISA, Military Services, DMS operations and maintenance commands, user communities, and individual users of the DMS.

DISA Circular 310-M70-89, "Defense Message System (DMS) Registration Procedures." This circular prescribes the policy and provides procedures for the registration of all users on the DMS high-grade services.

(INTENTIONALLY BLANK)

GLOSSARY

ABBREVIATIONS AND ACRONYMS

ACC	Area Control Center
ACP	Allied Communications Publication
ALDMSSTA	All DMS Stations
AN	Advisory Note
C&A	Certification and Accreditation
C/S/A	Combatant Commands, Services, and Agencies
CCEB	Combined Communications Electronics Board
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CMI	Classified Military Information
CSP	Common Security Protocol
C2	Command and Control
DAA	Designated Approving Authority
DADS	Defense Message System Asset Distribution System
DCID	Director, Central Intelligence, Directive
DIACAP	DOD Information Assurance Certification and Accreditation Process
DIAD	Defense Message System Integrated Architectural Database
DICAST	Defense And Intelligence Community Accreditation Support Team
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DMS	Defense Message System
DOD	Department of Defense

DoDD	Department of Defense Directive
DSA	Directory Service Agents
EAM	Emergency Action Message
EOS	Elements Of Service
FEN	Field Engineering Notice
FISMA	Federal Information Security Management Action
GENSER	General Service
GSM	Global Service Manager
HAG	High Assurance Guard
HS	Hybrid Solution
HTTP	Hypertext Transfer Protocol
IA	Information Assurance
IAVA	Information Assurance Vulnerability Alert
IC	Intelligence Community
IP	Interim Procedure
JITC	Joint Interoperability Test Command
JWICS	Joint Worldwide Intelligence Communication System
LCC	Local Control Centers
MIME	Multipurpose Internet Mail Extensions
MISSI	Multi-Level Information System Security Initiative
MFI	Multi-Function Interpreter
NATO	North Atlantic Treaty Organization
NC3	Nuclear Command, Control, and Communications
NetOps	Network Operations
NDP-1	National Disclosure Policy-1
NGCs	National Gateway Centers
NIPRNET	Non-Secure Internet Protocol Router Network

NOC	Network Operations Centers
NPES	Nuclear Planning and Execution System
NSA	National Security Agency
OPLAN	Operation Plan
OSD	Office of the Secretary of Defense
PKI	Public Key Infrastructure
PPS	Ports, Protocols, and Service
PUA	Proxy User Agent
SCI	Sensitive Compartmented Information
SIPRNET	Secret Internet Protocol Router Network
STANAG	Standardization Agreement
TC	Time Critical
TCP/IP	Transmission Control Protocol/Internet Protocol
TMG	Tactical Messaging Gateways
U.S.	United States
USMTF	U.S. Message Text Format
USSAN	United States Security Authority for NATO

(INTENTIONALLY BLANK)