CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6
DISTRIBUTION: A, B, C, S

CJCSI 5721.01G
1 July 2022

ORGANIZATIONAL MESSAGING SERVICE

References:
   See Enclosure D

1. <u>Purpose</u>. In accordance with (IAW) reference a, this instruction establishes policy and responsibilities for the use, operation, and management of the Defense Information Systems Agency (DISA) Organizational Messaging Service (OMS).

   a. Enclosure A outlines OMS policy.

   b. Enclosure B outlines the OMS mission and responsibilities.

   c. Enclosure C outlines the organizational structure of the OMS, to include the National Gateway Centers (NGCs) and their respective capabilities.

2. <u>Superseded/Cancellation</u>. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 5721.01F, "Organizational Messaging Service," February 2020, is hereby superseded."

3. <u>Applicability</u>. This policy applies to the Military Services and Defense Agencies subject to the direction of the CJCS and Combatant Commands (CCMDs) in the planning, operating, managing, and use of the organizational message processing systems that comprise the OMS. This instruction is available to other U.S. Government agencies and allied nations for information.

4. <u>Policy</u>. See Enclosure A.

5. <u>Definitions</u>. See Glossary.

6. <u>Responsibilities</u>. See Enclosure B.

7. <u>Summary of Changes.</u> CJCSI 5721.01G updates and supersedes the guidance in CJCSI 5721.01F. CJCSI 5721.01G minimizes the technical nature of CJCSI 5721.01F, focusing on the strategic impacts to users of the OMS. Significant improvements in CJCSI 5721.01G include:

    a. Transition from the Defense Messaging System to a fee-for-service OMS.

    b. Clarification of new organizational responsibilities as it relates to the OMS.

    c. Streamlining and updating relevant references and definitions.

    d. Updating security reference guidelines from the Department of Defense (DoD) Risk Management Framework (RMF).

8. <u>Releasability.</u> UNRESTRICTED. This directive is approved for public release; distribution is unlimited on NIPRNET. DoD Components (to include the CCMDs), other Federal agencies, and the public, may obtain copies of this directive through the Internet from the CJCS Directives Electronic Library at <http://www.jcs.mil/library>. Joint Staff activities may also obtain access via the SIPR directives Electronic Library websites.

9. <u>Effective Date.</u> This INSTRUCTION is effective upon receipt.

For the Chairman of the Joint Chiefs of Staff:

GEORGE M. WIKOFF, RADM, USN
Vice Director, Joint Staff

Enclosures
  A – Policy
  B – Mission and Responsibilities
  C – Organizational Structure and Capabilities
  D – References
  GL – Glossary

DISTRIBUTION

Distribution A, B, C plus the following:

"OPR for the subject directive has chosen electronic distribution to the above organizations via E-mail. The Joint Staff Information Management Division has responsibility for publishing the subject directive to the SIPR and NIPR Joint Electronic Library web sites."

(INTENTIONALLY BLANK)

CJCSI 5721.01G
1 July 2022

ENCLOSURE A

POLICY

1. <u>Organizational Message Service Policy</u>. OMS policy establishes the guidelines to exchange organizational messages within and between the DoD, the U.S. Intelligence Community (IC), other U.S. Government Agencies, and U.S. allies.

    a. OMS is the DoD system of record for all organizational message traffic.

    b. OMS provides a range of assured services to the customer community that includes the Military Services, DoD Agencies, CCMDs, non-DoD U.S. government activities, and the Intelligence Community (IC).

    c. OMS supports the assured secure delivery of organizations' messages and includes the ability to exchange official information between military organization and to support interoperability between allied nations, non-DoD activities, and the IC.

    d. OMS information, to include features, billing rates, and service support is located on the DISA website: <https://www.disa.mil/Network-Services/Organizational-Messaging-Service>. Further information regarding the OMS mission and responsibilities is located in Enclosure B.

    e. OMS is a customer reimbursable service that facilitates the exchange of official information between the customer communities. Rates are located through the Mission Partner Portal:<https://disa.deps.mil /ext/cop/mpp/index.aspx>.

    f. DoD electronic messaging services must operate in compliance with OMB Memorandum M-10-23.

2. <u>The Office of the Secretary of Defense (OSD)</u>

    a. Develops and coordinates DoD issuances for policy on the use, risk management, and compliance of official DoD information online, electronic messaging, and electronic messaging services.

    b. Provides records management guidance and oversight for the use of online information and electronic messaging, in accordance with DoD Directive (DoDD) 5144.02.

   c. Approves U.S. Government non-DoD organizations requesting access to the OMS. Requestors must have the capability to access the DoD Information Network (DoDIN) for any connecting systems.

   d. Considers connection requests if the requestor cannot satisfy their requirement by other means, the requirement supports a DoD mission, and if a DoD activity sponsors the request or the requestor has prior OSD approval. DISA may consider non-U.S. activities for OMS access pending OSD approval. Requests are processed under the provisions of reference a.

3. National Disclosure Policy-1 (NDP-1)

   a. The National Security Council with the approval of the President established reference b, governs disclosure of classified military information (CMI) to foreign governments.

   b. The disclosure of CMI to foreign governments and international organizations is limited and is IAW references b and c.

4. OMS Framework. OMS provides a framework for messaging systems to connect to exchange organizational messages using a suite of available OMS connection options and a shared directory. The architecture does not limit how a connecting message system will support its local users and the distribution of its received messages or the handling of originating messages prior to their transmission through OMS.

5. Security. Security authorizations to operate are IAW the DoD RMF (reference d) and are the joint responsibility of the DoDIN authorizing officials. OMS systems connecting to U.S. IC networks are IAW the IC RMF (references d and e). Systems connecting to OMS will follow their local security guidelines. In some cases, connecting systems may use the OMS authorization to operate as a reciprocal artifact. The OMS NGCs follow security guidance outlined in the DoD security directives (references d, e, f, and g).

ENCLOSURE B

MISSION AND RESPONSIBILITIES

1. <u>The Organizational Messaging Service (OMS) Mission/Responsibilities</u>. The OMS derives its primary mission and responsibilities from reference a, which establishes the doctrinal foundation for communications system support of joint procedures across the range of military operations.

2. <u>The Organizational Messaging Service (OMS) Mission</u>. The OMS is a fee for service capability which provides a range of assured messaging and directory services to the Military Services, DoD Agencies, CCMDs, non-DoD U.S. Government activities, the U.S. IC, and North Atlantic Treaty Organization (NATO)/Allied Mission Partners as illustrated in Figure 1, to empower secured military messaging interoperability (references c and i).

Figure 1. OMS Operational View

Organizational Messaging (OM) supports the secure delivery of organizational messages within strict service parameters and provides reach back capability for strategic, fixed-base, and tactical deployed environments. The OMS:

a. Provides the capability to exchange official information between interconnected OM communities using a variety of end-user systems, message formats, and transport protocols;

b. Delivers command and control (C2) messaging capabilities supporting timely, secure, reliable and authoritative message exchanges between OMS messaging communities;

c. Supports end-user system connections from UNCLASSIFIED to TOP SECRET/COLLATERAL/SENSITIVE COMPARTMENTED INFORMATION (reference j); and

d. Consists of all hardware, software, policy, procedures, standards, facilities, and personnel necessary to support the exchange of messages and attachments.

3. The Organizational Messaging Service (OMS) Responsibilities. Organizational messages comprise official information including C2, cyber, and intelligence communications between organizational elements connected to the OMS. All messages require prior approval for release by an originating organization and determination of distribution by the receiving organization.

a. Joint Staff

(1) Serves as approval authority for declaring Emergency Action Message (EAM) messaging processing systems acceptable and the system of record for EAM dissemination.

(2) Develops policy and guidance for products, architectures, configurations, and capabilities IAW messaging policy, security, and governance.

b. Military Services, Department of Defense Agencies, and Combatant Commands. Operate, maintain, and provide network access to any locally hosted message handling system supporting end-users on base, post, camp or station.

c. Local Site Messaging System Operational/Program Manager

(1) Manages the site's implementation, configuration, operation, and maintenance of the local message handling system;

(2) Coordinates testing with DISA and validates continued interoperability prior to implementation; and

(3) Addresses shortfalls in messaging interoperability with the OMS to their executive agents and/or component commands.

d. <u>Defense Information Systems Agency (DISA)</u>. Serves as lead agency with mission responsibility for the design, implementation, integration, operational direction, and management control over all core elements of the OMS as part of the DoDIN. DISA implements and sustains the communications gateway infrastructure and sustains the DoD OMS for automated messaging between CCMDs, Services, and agencies using global addressing and routing via the NGC (References b, h, and k).

(1) Provides testing of OMS key components to ensure functional, security, and interoperability requirements are validated prior to release to Joint Interoperability Test Command for testing; and

(2) Provides representation to the Combined Communications-Electronic Boards (CCEBs) Message Working Group to maintain, coordinate, and ensure maintenance of message system interoperability.

e. <u>Joint Interoperability Test Command</u>. Provides government certification and integration and operational testing of core OMS components prior to implementation of the full operational capability (reference k).

(INTENTIONALLY BLANK)

CJCSI 5721.01G
1 July 2022

ENCLOSURE C

ORGANIZATIONAL STRUCTURE AND CAPABILITIES

1. <u>The Organizational Messaging System (OMS) National Gateway Centers (NGCs)</u>. There are three gateway message-switching centers to which OMS subscribers connect to for the capability to exchange messages.

    a. NGC located in Ft Detrick, Maryland (NGC-D)

    b. NGC located in the Pentagon Telecommunications System Center in Arlington, Virginia (NGC-P)

    c. NGC at Raven Rock Mountain Complex (NGC-RRMC)

2. <u>National Gateway Center's (NGCs) Capabilities</u>. All three NGCs are active and logically coupled to provide a common set of transports, shared directory, and a routing backbone. This ensures end-user systems can transmit and receive organizational messages to all connected messaging communities, including those in the joint environment (reference a). The NGCs provide and support the following OMS capabilities:

    a. Replicated authoritative directory system between all NGCs.

        (1) The directory is shared with the messaging communities including allied messaging systems; and

        (2) The shared directory allows the exchange and conversion of messages as necessary, by OMS to support the connecting messaging systems requirements.

    b. Network connectivity from the NGCs to all Military Services/CCMDs, U.S. IC, U.S. Allies, and other U.S. Government agency messaging systems (reference c).

    c. Actively managed centralized gateway capability distributed between the three NGCs. The gateway supports transport protocol conversion and routing between the various connecting systems. This includes supporting U.S. Message Text Format (USMTF) embedded within the body-text of OMS supported formats. The DoD end-user messaging systems provide a USMTF editor (Reference g).

d. Daily creation and exchange of multiple directory extract formats used by other messaging systems connecting to OMS.

e. Releasable and eyes-only message handling.

f. Content routing and distribution based on parsed or semi-structured format fields, keywords and phrases, and search capabilities of consolidated message archives.

g. Organizational message auditing and tracing within the OMS to provide non-repudiation of the sending organization.

h. A high-level of service availability based on multiple NGCs, redundant equipment, multiple communication paths, and continuity of operations sites and managed alternate site routing plans.

ENCLOSURE D

REFERENCES

a. JP 6-0, "Joint Communication System," 10 June 2015, Incorporating change 1, 4 October 2019.

b. NDP-1, "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations," 2 October 2000, as amended."

c. CJCSI 6740.01C "Military Telecommunications Agreements and Arrangements Between the United States and Regional Defense Organizations or Friendly Foreign Nations," 17 June 2019."

d. DoDD 5200.1-R, "DoD Information Security Program," 19 March 2013

e. DoDD 5200.2-R "Procedures for the DoD Personnel Security Program (PSP)," 3 April 2017

f. ICD 503, "Intelligence Community Information Technology Systems Security Risk Management," 21 July 2015

g. CJCSI 6241.04D, "Policy and Procedures for Management and Use of United States Message Text Formatting," 12 January 2021."

h. DISA IE Directorate, "Telecommunications Service Level Agreement (SLA)," 9 December 2016

i. CJCSI 5221.01E, "Delegation of Authority to Commanders of Combatant Commands to Disclose Classified Military Information to Foreign Governments and International Organizations," 15 December 2021."

j. ICD 703, "Protection of Classified National Intelligence, Including Sensitive Compartmented Information," 21 June 2013

k. CJCSI 6211.02D, "Defense Information System Network (DISN) Responsibilities," 4 August 2015.

SUPPORTING DOCUMENTATION

1. DoDD 5105.19, "Defense Information System Agency (DISA)," 15 February 2022."

2. DoDI 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," 12 March 2014, Incorporating change 3, 29 December 2020.

3. DoDI 8170.01 "Online Information Management and Electronic Messaging," 2 January 2019, Change 1, 24 August 2021.

GLOSSARY

PART I – ACRONYMS

C2	Command and Control
CCMD	Combatant Command
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joints Chiefs of Staff Instruction
CCEB	Combined Communications-Electronic Board
CMI	Classified Military Information
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoDIN	Department of Defense Information Network
EAM	Emergency Action Message
IAW	in accordance with
IC	Intelligence Community
ICD	Intelligence Community Directive
JP	Joint Publication
NATO	North Atlantic Treaty Organization
NC3	Nuclear Command, Control, and Communications
NDP-1	National Disclosure Policy-1
NGC	National Gateway Center
OM	Organizational Messaging
OMS	Organizational Messaging Service
OSD	Office of the Secretary of Defense
RMF	Risk Management Framework
TS	Top Secret
USMTF	U.S. Message Text Format

PART II – DEFINITIONS

Unless otherwise stated, the terms and definitions contained in this glossary are for the purposes of this instruction only.

Allied Communication Publication. A series of publications developed by the CCEB and NATO containing Allied military information that define communications procedures that can be used by an appropriate implementing agency to ensure interoperability.

Automated Message Handling System. Messaging system that provides OMS users with an interface for receiving and originating organizational messages.

Emergency Action Message. Highest message priority processed by OMS to support Nuclear Command, Control, and Communications (NC3) operations with a time objective of 2 minutes or less.

Intelligence Community (IC) Information Transport Service. Provides the IC with a common set of services, architectural infrastructure, operating environment, and maintenance support to seamlessly transport information across IC-unique domains and via cross domain systems to other domains such as the DoD and U.S. government agencies. Specifically, the ITS supports the transfer of multiple data classes to include near real-time messages, organizational messages, bulk data, and intelligence products. (ITS Interface Control Document)

Interoperability

   a. The ability to operate in synergy in the execution of assigned tasks. (JP 3-0)

   b. The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. (JP 6-0)

Management Threshold. Management thresholds are numerical baselines against which operational performance is measured to highlight where management action is required (reference h).

Organizational Messaging Service. Provides a range of assured services to the customer community that include the Military Services, DoD agencies, CCMDs, non-DoD U.S. government agencies, and the IC. These services include the ability to exchange official information between military organizations and to

support interoperability with allied nations, non-DoD activities and the IC operating in both the strategic/fixed-base and tactical/deployed environments.

<u>Plain Language Address Expansion</u>. In OMS, the group expansion of an Address Indicator Groups (AIG), Task Force (TF) or a Collective Address Designator (CAD) to PLA members of the group.

(INTENTIONALLY BLANK)