

UNCLASSIFIED



**CHAIRMAN OF THE JOINT
CHIEFS OF STAFF
INSTRUCTION**

J-6

DISTRIBUTION: A, B, C, S

CJCSI 5721.01H

14 March 2025

ORGANIZATIONAL MESSAGING SERVICE

References:

See Enclosure D

1. Purpose. 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). This includes OMS policy, mission, and responsibilities, and the organizational structure of the OMS, to include the National Gateway Centers (NGCs) and their respective capabilities.
2. Superseded/Cancellation. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 5721.01G, "Organizational Messaging Service," 1 July 2022 is hereby superseded.
3. Applicability. 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. Policy. See Enclosure A.
5. Definitions. See Glossary.
6. Responsibilities. See Enclosure B.
7. Summary of Changes. This instruction has been revised to update the references list and distribution, and to verify the links used in the policy.
8. Releasability. UNRESTRICTED. This directive is approved for public release; distribution is unlimited on the Non-classified Internet Protocol Router Network (NIPRNET). DoD Components (to include the CCMDs), other Federal

UNCLASSIFIED

UNCLASSIFIED

CJCSI 5721.01H

14 March 2025

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 SECRET Internet Protocol Router Network (SIPRNET) directives Electronic Library web sites.

9. Effective Date. This INSTRUCTION is effective upon signature.

For the Chairman of the Joint Chiefs of Staff:



STEPHEN E. LISZEWSKI, MajGen, USMC
Vice Director, Joint Staff

Enclosures

- A – Policy
- B – Mission and Responsibilities
- C – Organizational Structure and Capabilities
- D – References

UNCLASSIFIED

CJCSI 5721.01H
14 March 2025

DISTRIBUTION

Distribution A, B, C, S plus the following:

Commander, U.S. Element North American Aerospace Defense Command
Commander, Joint Interoperability Test Command
U.S. Representative to the Military Committee to NATO Liaison Office
U.S. Liaison Officer to Supreme Allied Commander, Transformation
Office of Director of National Intelligence / Chief Information Officer

The office of primary responsibility 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 SIPRNET and NIPRNET Joint Electronic Library web sites.

UNCLASSIFIED

UNCLASSIFIED

CJCSI 5721.01H
14 March 2025

(INTENTIONALLY BLANK)

UNCLASSIFIED

ENCLOSURE A

POLICY

1. OMS Policy. OMS policy establishes the guidelines to exchange organizational messages within and between the DoD, the U.S. Intelligence Community (IC), other U.S. Government (USG) agencies, and U.S. allies.
 - a. OMS is the DoD's 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 USG activities, and the IC.
 - c. OMS supports the assured secure delivery of organizational messages and includes the ability to exchange official information between military organizations and to support interoperability between allied nations, non-DoD activities, and the IC.
 - d. OMS provides the capability to exchange official information between interconnected organizational messaging communities using a variety of end-user systems, message formats, and transport protocols.
 - e. OMS delivers command and control (C2) messaging capabilities supporting timely, secure, reliable, and authoritative message exchanges between OMS messaging communities.
 - f. OMS supports end-user system connections from UNCLASSIFIED, SECRET, and TOP SECRET enclaves, to include compartmentalized connections (reference (b)).
 - g. OMS consists of all hardware, software, policies, procedures, standards, facilities, and personnel necessary to support the exchange of messages and attachments.
 - h. OMS information—to include features, billing rates, and service support—is located on the DISA web site at <<https://www.disa.mil/Network-Services/Organizational-Messaging-Service>>. Further information regarding the OMS mission and responsibilities is located in Enclosure B.
 - i. 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://services.disa.mil/csm?id=kb_article_view&sys_kb_id=220cad4397c71a54870273c11153afc5>.

j. DoD electronic messaging services must operate IAW reference (c).

2. The Office of the Secretary of Defense

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 IAW reference (d).

c. Approves non-DoD USG 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 either a DoD activity sponsors the request or the requestor has prior Office of the Secretary of Defense (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

a. The National Security Council, with the approval of the President, established National Disclosure Policy-1 (NDP-1). The NDP-1 is only available on a need-to-know basis and governs disclosure of classified military information (CMI) to foreign governments. Reference (e) is the governing policy on CMI for the DoD.

b. The disclosure of CMI to foreign governments and international organizations is limited. Refer to references (e) and (f) for policy and responsibility regarding disclosure.

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 reference (g) and are the joint responsibility of the DoDIN authorizing officials. OMS systems connecting to IC networks are IAW the references (h) and (i). Systems

UNCLASSIFIED

CJCSI 5721.01H

14 March 2025

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 references (h)–(k).

UNCLASSIFIED

CJCSI 5721.01H
14 March 2025

(INTENTIONALLY BLANK)

UNCLASSIFIED

ENCLOSURE B

MISSION AND RESPONSIBILITIES

1. OMS Mission. 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. It is a fee-for-service capability that provides a range of assured messaging and directory services to the Military Services, DoD agencies, CCMDs, non-DoD USG activities, IC, and North Atlantic Treaty Organization (NATO)/Allied Mission Partners as illustrated in Figure 1 to empower secured military messaging interoperability (references (f) and (l)).



Figure 1. OMS Operational View

2. 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.

UNCLASSIFIED

CJCSI 5721.01H

14 March 2025

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 instruction.

b. Military Services, DoD 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.

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

d. Defense Information Systems Agency. 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 (e), (m), and (n)).

(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.

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

UNCLASSIFIED

CJCSI 5721.01H

14 March 2025

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

UNCLASSIFIED

CJCSI 5721.01H
14 March 2025

(INTENTIONALLY BLANK)

B-4

Enclosure B

UNCLASSIFIED

ENCLOSURE C

ORGANIZATIONAL STRUCTURE AND CAPABILITIES

1. The OMS National Gateway Centers. There are three gateway message-switching centers to which OMS subscribers connect to:
 - a. NGC-D is located in Ft Detrick, Maryland.
 - b. NGC-P is located in the Pentagon Telecommunications System Center in Arlington, Virginia.
 - c. NGC-RRMC is located at Raven Rock Mountain Complex.
2. NGC Capabilities. 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.
 - (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, the IC, U.S. allies, and other USG agency messaging systems (reference (f)).
 - 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 (k)).
 - 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.

UNCLASSIFIED

CJCSI 5721.01H
14 March 2025

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.

UNCLASSIFIED

CJCSI 5721.01H
14 March 2025

ENCLOSURE D

REFERENCES

- a. JP 6-0, 4 December 2023, *Joint Communications*
- b. ICD 703, 21 June 2013, “Protection of Classified National Intelligence, Including Sensitive Compartmented Information”
- c. OMB memo M-10-23, 25 June 2010, “Guidance for Agency Use of Third-Party Websites and Applications”
- d. DoDD 5144.02, 21 November 2014 incorporating change 19 September 2017, “DoD Chief Information Officer (DoD CIO)”
- e. DoDD 5230.11, 7 November 2023, “Disclosure of Classified Military Information to Foreign Governments and International Organizations”
- f. CJCSI 6740.01D, 17 April 2023, “Military Telecommunications Agreements and Arrangements Between the United States and Regional Defense Organizations or Friendly Foreign Nations”
- g. DoDI 8510.01, 19 July 2022, “Risk Management Framework (RMF) for DoD Systems”
- h. DoDM 5200.01 Volume 3, 24 February 2012 incorporating Change 3, 28 July 2020, “DoD Information Security Program: Protection of Classified Information”
- i. DoDI 5200.02, 21 March 2014 incorporating Change 3, 24 September 2020, “DoD Personnel Security Program (PSP)”
- j. ICD 503, 25 October 2024, “Intelligence Community Information Environment Risk Management”
- k. CJCSI 6241.04E, 7 October 2023, “Policy and Procedures for Management and Use of United States Message Text Formatting”
- l. CJCSI 5221.01E, 15 December 2021, “Delegation of Authority to Commanders of Combatant Commands to Disclose Classified Military Information to Foreign Governments and International Organizations”
- m. DISA Defense Working Capital Fund Services, 2 June 2023, “Service Level Document (SLD) between Defense Information Systems Agency (DISA) and DISA-Organizational Messaging Service (OMS)”

UNCLASSIFIED

UNCLASSIFIED

CJCSI 5721.01H

14 March 2025

n. CJCSI 6211.02D, 4 August 2015, “Defense Information System Network (DISN) Responsibilities”

SUPPORTING DOCUMENTATION

1. DoDD 5105.19, 15 February 2022, “Defense Information System Agency (DISA)”
2. DoDI 8170.01, 2 January 2019 incorporating Change 1, 24 August 2021, “Online Information Management and Electronic Messaging”

GLOSSARY

PART I – ACRONYMS AND ABBREVIATIONS

C2	command and control
CCMD	Combatant Command
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joints Chiefs of Staff Instruction
CMI	classified military information
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoDIN	Department of Defense Information Network
EAM	Emergency Action Message
IAW	in accordance with
IC	Intelligence Community
ITS	Information Transport Service
NATO	North Atlantic Treaty Organization
NDP-1	National Disclosure Policy-1
NGC	National Gateway Center
NIPRNET	Non-classified Internet Protocol Router Network
OMS	Organizational Messaging Service
OSD	Office of the Secretary of Defense
SIPRNET	SECRET Internet Protocol Router Network
USG	U.S. Government
USMTF	U.S. Message Text Format

UNCLASSIFIED

CJCSI 5721.01H
14 March 2025

(INTENTIONALLY BLANK)

UNCLASSIFIED

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 Combined Communications-Electronic Board and North Atlantic Treaty Organization 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 Organizational Messaging Service users with an interface for receiving and originating organizational messages.

cyber communication. The exchange of information in and through cyberspace.

Emergency Action Message. Highest message priority processed by Organizational Messaging Service to support Nuclear Command, Control, and Communications operations with a time objective of 2 minutes or less.

Intelligence Community Information Transport Service. Provides the Intelligence Community (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 Department of Defense and U.S. government agencies. Specifically, the Information Transport Service 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. (DoDM 5200.01 V3).

UNCLASSIFIED

CJCSI 5721.01H

14 March 2025

Organizational Messaging Service. Provides a range of assured services to the customer community, which includes the Military Services, Department of Defense (DoD) agencies, Combatant Commands, non-DoD U.S. government agencies, and the Intelligence Community (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.

Plain Language Address Expansion. In the Organizational Messaging Service, the group expansion of an Address Indicator Group, Task Force, or a Collective Address Designator to plain language address members of the group.