



Department of Defense INSTRUCTION

NUMBER 8260.03

February 19, 2014

Incorporating Change 1, Effective March 19, 2018

USD(P&R)

SUBJECT: The Global Force Management Data Initiative (GFM DI)

References: See Enclosure 1

1. PURPOSE. This instruction:

a. Reissues DoD Instruction (DoDI) 8260.03 (Reference (a)) in accordance with the authority in DoD Directive (DoDD) 5124.02 (Reference (b)) to establish policy, assign responsibilities, and prescribe procedures for the GFM DI.

b. Mandates the GFM DI to develop standardized enterprise force structure data, available electronically in a joint hierarchical way for integration and use throughout the DoD, to achieve the net-centric vision of Strategic Planning Guidance (Reference (c)).

2. APPLICABILITY. This instruction applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combat Commands (CCMDs), the Office of the Inspector General of the Department of Defense (IG DoD), the Defense Agencies, the DoD Field Activities, the National Guard Bureau, and all other organizational entities within the DoD (referred to collectively in this instruction as the "DoD Components").

3. POLICY. It is DoD policy that:

a. Information is a strategic asset to the DoD. It must be appropriately secured, shared, and made available throughout the information life cycle to any DoD user or mission partner to the maximum extent allowed by law and DoD policy, pursuant to DoDD 8000.01 (Reference (d)), DoDI 8320.02 (Reference (e)), ~~DoDD~~ *DoDI* 8320.03 (Reference (f)), the DoD Chief Information Officer (DoD CIO) Capability Planning Guidance for Fiscal Years 2014-2018 (Reference (g)), DoD Standard 5015.02 (Reference (h)), and supplementary DoD component records and information management issuances.

b. The GFM DI, guided by a collaborative community of interest (COI), must provide a digitized, hierarchical, enterprise force structure baseline with billet level resolution of all

authorized forces, organizational elements, and crewed platforms in the DoD, for end-to-end data integration across the DoD functional areas.

c. The enterprise force structure baseline must:

(1) Be populated and maintained in accordance with GFM DI technical guidance by the DoD Components in organization (“org”) servers.

(2) Be generated in org servers in a security domain commensurate with the classification handling of the data produced.

(3) Be replicated in the org servers of subsequently higher security domains for augmentation with data of greater classification.

(4) Consist of every organizational element in the DoD, including all unit, crew, and billet authorization data, and the authorization inventory for crewed platforms and beyond line-of-sight unmanned aerial vehicles.

(5) Be shared with any DoD user or mission partner to the maximum extent allowed by law and DoD policy for use as a common reference for information technology (IT) systems, enhancing functional information capabilities in support of the joint information environment.

(6) Be used in DoD IT systems to the lowest tactical level technically feasible for any DoD force structure representation applicable to that system, providing the framework for integration of authorization data and authorization inventory with actual organizations, equipment, and personnel (including associated resource, readiness, and capability information), and enabling identity management and secure data access.

4. RESPONSIBILITIES. See Enclosure 2.

5. PROCEDURES. See Enclosure 3.

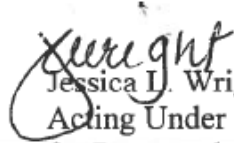
6. RELEASABILITY. ~~Unlimited. This instruction is approved for public release and is available on the Internet from the DoD Issuances Website at <http://www.dtic.mil/whs/directives>. Cleared for public release. This instruction is available on the Directives Division Website at <http://www.esd.whs.mil/DD/>.~~

7. EFFECTIVE DATE. This instruction ~~is effective February 19, 2014.~~

~~a. Is effective February 19, 2014.~~

~~b. Must be reissued, cancelled, or certified current within 5 years of its publication to be considered current in accordance with DoD Instruction 5025.01 (Reference (i)).~~

~~e. Will expire effective February 19, 2024 and be removed from the DoD Issuances Website if it hasn't been reissued or cancelled in accordance with Reference (i).~~


Jessica L. Wright
Acting Under Secretary of Defense
for Personnel and Readiness

Enclosures

1. References
2. Responsibilities
3. Procedures

Glossary

TABLE OF CONTENTS

ENCLOSURE 1: REFERENCES.....5

ENCLOSURE 2: RESPONSIBILITIES.....7

 UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS
 (USD(P&R)).....7

 DIRECTOR, DEPARTMENT OF DEFENSE HUMAN RESOURCES ACTIVITY
 (DoDHRA)8

~~DEPUTY~~ CHIEF MANAGEMENT OFFICER OF THE DEPARTMENT OF DEFENSE
 (~~DCMO~~).....9

 UNDER SECRETARY OF DEFENSE FOR ACQUISITION, ~~TECHNOLOGY,~~ AND
 ~~LOGISTICS~~ SUSTAINMENT (USD(~~AT&L~~ A&S))9

 USD(I).....10

 DoD CIO.....11

 DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA)11

 OSD AND DoD COMPONENT HEADS.....12

 SECRETARIES OF THE MILITARY DEPARTMENTS.....12

 CJCS13

 CCDRs15

 CHIEF, NGB.....15

ENCLOSURE 3: PROCEDURES.....16

 GFM DI GOVERNANCE.....16

 ORG SERVER PROCEDURES AND REQUIREMENTS16

GLOSSARY21

 PART I: ABBREVIATIONS AND ACRONYMS21

 PART II: DEFINITIONS.....22

TABLE

 The Component Org Servers17

ENCLOSURE 1

REFERENCES

- (a) DoD Instruction 8260.03, "Organizational and Force Structure Construct (OFSC) for Global Force Management (GFM)," August 23, 2006 (hereby cancelled)
- (b) DoD Directive 5124.02, "Under Secretary of Defense for Personnel and Readiness (USD(P&R))," June 23, 2008
- (c) Deputy Secretary of Defense Memorandum, "Strategic Planning Guidance Fiscal Years 2006-2011," March 15, 2004¹
- ~~(d) DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise," February 10, 2009~~
- (d) DoD Directive 8000.01, "Management of The Department of Defense Information Enterprise (DoD IE)," March 17, 2016, as amended*
- (e) DoD Instruction 8320.02, "Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense," August 5, 2013
- ~~(f) DoD Directive 8320.03, "Unique Identification (UID) Standards for a Net Centric Department of Defense," March 23, 2007~~
- (f) DoD Instruction 8320.03, "Unique Identification (UID) Standards for Supporting DoD Net-Centric Operations," November 4, 2015*
- (g) DoD Chief Information Officer Capability Planning Guidance for Fiscal Years 2014-2018, February 17, 2012²
- (h) DoD 5015.02-STD, "Electronic Records Management Software Applications Design Criteria Standard," April 25, 2007
- ~~(i) DoD Instruction 5025.01, "DoD Directives Program," September 26, 2012, as amended~~
- (j) DoD Instruction 8115.02, "Information Technology Portfolio Management Implementation," October 30, 2006
- ~~(k) DoD 8320.02-G, "Guidance for Implementing Net-Centric Data Sharing," April 12, 2006~~
- (k) DoD Instruction 8320.07, "Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense," August 3, 2015*
- (l) DoD 8260.03-M, Volume 1, "Global Force Management Data Initiative (GFM DI) Implementation: Unique Identification (UID) for GFM," November 20, 2009
- (m) DoD 8260.03-M, Volume 2, "Global Force Management Data Initiative (GFM DI) Implementation: The Organizational and Force Structure Construct (OFSC)," June 14, 2011
- (n) Joint Requirements Oversight Council, "Capability Development Document for Global Force Management Data Initiative, Increment 1," January 28, 2008³
- ~~(o) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003~~
- (o) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014*

¹ This document is classified and not releasable to the public. Individuals may request access to this document from the Office of the Under Secretary of Defense for Policy, through the Heads of their OSD Components.

² This document is For Official Use Only and not releasable to the public. Individuals may request access to this document from the Office of the DoD CIO.

³ Copies may be obtained from the DoD NIPRNET Intellipedia at https://www.intelink.gov/wiki/Global_Force_Management_Data_Initiative/CCB

- (p) DoD Instruction 8510.01, “DoD Information Assurance Certification and Accreditation Process (DIACAP),” November 28, 2007
- (q) DoD Instruction 5200.39, “Critical Program Information (CPI) Protection Within the Department of Defense,” July 16, 2008, as amended
- ~~(r) DoD Directive 4630.05, “Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS),” May 5, 2004, as amended~~
- (r) *DoD Instruction 8330.01, “Interoperability of Information Technology (IT), Including National Security Systems (NSS),” May 21, 2014*
- (s) Chairman of the Joint Chiefs of Staff Instruction 6212.01F, “Net Ready Key Performance Parameter (NR KPP),” March 21, 2012
- (t) DoD Manual 5200.01, Volumes 1-4, “DoD Information Security Program,” February 24, 2012, as amended
- (u) Secretary of Defense Memorandum, “Guidance for the Employment of the Force,” current edition¹
- (v) Secretary of Defense Memorandum, “Global Force Management Implementation Guidance, current edition¹
- ~~(w) DoD Directive 5400.11, “DoD Privacy Program,” May 8, 2007, as amended~~
- (v) *DoD Directive 5400.11, “DoD Privacy Program,” October 29, 2014*
- (xw) DoD 5400.11-R, “Department of Defense Privacy Program,” May 14, 2007
- (yx) Title 10, United States Code
- (zy) DoD Instruction 8320.04, “Item Unique Identification (IUID) Standards for Tangible Personal Property,” June 16, 2008
- ~~(aa) DoD Instruction 4165.14, “Real Property Inventory (RPI) and Forecasting,” March 31, 2006~~
- (aa) *DoD Instruction 4165.14, “Real Property Inventory (RPI) and Forecasting,” January 17, 2014*
- ~~(ab) DoD Directive 5143.01, “Under Secretary of Defense for Intelligence (USD(I)),” November 23, 2005~~
- (ab) *DoD Directive 5143.01, “Under Secretary of Defense for Intelligence (USD(I)),” October 24, 2014, as amended*
- (ac) DoD Directive 5105.19, “Defense Information Systems Agency (DISA),” July 25, 2006
- (ad) DoD Instruction 5105.18, “DoD Intergovernmental and Intragovernmental Committee Management Program,” July 10, 2009, as amended
- (ae) Joint Publication 1, “Doctrine for the Armed Forces of the United States,” *current edition March 25, 2013*
- ~~(af) Joint Publication 1-02, “Department of Defense Dictionary of Military and Associated Terms,” current edition~~
- (af) *Office of the Chairman of the Joint Chiefs of Staff, “DoD Dictionary of Military and Associated Terms,” current edition*
- (ag) Committee on National Security Systems Instruction 4009, “National Information Assurance (IA) Glossary,” April 26, 2010⁴
- (ah) DoD Instruction 1000.30, “Reduction of Social Security Number (SSN) Use Within DoD,” August 1, 2012

⁴ Documents issued by the Committee on National Security Systems (CNSS) are available at <https://www.cnss.gov/cnss/index.cfm>

- (ai) DoD Directive 5100.01, "Functions of the Department of Defense and Its Major Components," December 21, 2010

ENCLOSURE 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS

(USD(P&R)). In addition to the responsibilities in section 8 of this enclosure, the USD(P&R):

- a. Develops supporting guidance, as necessary, for implementation of this instruction.
- b. Provides representation to GFM DI governance bodies.
- c. Validates GFM DI policy and artifacts in collaboration with the CJCS and the OSD and DoD Component heads.
- d. Pursuant to the procedures detailed in Enclosure 3 of this instruction, and in cooperation with the OSD Component heads and the directors of the Defense Agencies and DoD Field Activities that fall under the authority, direction, and control of an OSD Component:
 - (1) Provides management and oversight for the integrated population and maintenance of an OSD Org Server (OSDOS) that:
 - (a) Documents the relatively permanent placement of all force structure within OSD Components and the Defense Agencies and DoD Field Activities that report to them, except for those Defense Intelligence organizations described in section 5 of this enclosure:
 - (b) Exists on both the Non-Secure Internet Protocol Router Network (NIPRNET) and SECRET Internet Protocol Router Network (SIPRNET).
 - (c) Replicates in the SIPRNET OSDOS all data in the NIPRNET OSDOS for augmentation with classified data.
 - (2) Deconflicts efforts, as necessary, with the Under Secretary of Defense for Intelligence (USD(I)) and the CJCS, in coordination with the Director of Administration and Management.
 - (3) Manages investments for OSDOS development and maintenance pursuant to DoDI 8115.02 (Reference (j)).
 - (4) Publishes the pedigree, security level, and access control level of OSDOS data through the applicable registries pursuant to ~~DoD 8320.02-G~~ *DoDI 8320.07* (Reference (k)).
 - (5) Provides OSDOS functionality pursuant to GFM DI technical guidance, including DoD Manual 8260.03-M, Volumes 1 and 2 (References (l) and (m), respectively), and the GFM DI Increment 1 Capability Development Document (Reference (n)).

(6) Exposes OSDOS data to external consumer systems in compliance with:

(a) References (d), (e), (f), and (g) regarding sharing and management of enterprise information.

(b) ~~DoDI 8500.2~~ *DoDI 8500.01* (Reference (o)), 8510.01 (Reference (p)), and 5200.39 (Reference (q)) regarding information assurance (IA) and protection.

(c) ~~DoDD 4630.05~~ *DoDD 8330.01* (Reference (~~q~~)) and CJCS Instruction 6212.01 (Reference (~~q~~)) regarding interoperability and Net Ready Key Performance Parameters (NR KPP) requirements.

(d) Volumes 1 through 4 of DoD Manual 5200.01 (Reference (~~ts~~)), regarding classified and controlled unclassified information.

(7) Publishes, from both the NIPRNET and SIPRNET OSDOS:

(a) The file of reference data common to all of the DoD Components, that includes reference data specific to OSD Components and the organizations they control, for use by data consumers, including other org servers, that contain billets from those organizations.

(b) The file of upper echelon force structure data common to all of the DoD Components, known as the Bridge, as described in section 18 of Reference (m).

(8) Documents and manages joint billets and joint billet organization unique identifiers (OUIDs) pursuant to Reference (l) and paragraph 2d(3) of Enclosure 3 of this instruction.

(9) In coordination with the OSD Component heads and directors of the Defense Agencies and DoD Field Activities, fully supports the transition to a force management process that enables the global sourcing of operational needs, pursuant to Reference (c), and the Secretary of Defense Memorandums Guidance for Employment of the Force (Reference (u)), and Global Force Management Implementation Guidance (Reference (v)).

2. DIRECTOR, DEPARTMENT OF DEFENSE HUMAN RESOURCES ACTIVITY (DoDHRA). Under the authority, direction, and control of the USD(P&R), through the Director, Defense Manpower Data Center (DMDC), the Director, DoDHRA:

a. Establishes the enterprise repository for the authoritative linkage between enterprise force structure, to include billet-level OUIDs, and the electronic data interchange personal identifier (EDI-PI) of the individuals serving in those billets.

b. Coordinates fully with the DoD Components to expose enterprise repository data to consumer systems, in compliance with:

(1) References (d), (e), (f), and (g) regarding sharing and management of enterprise information.

(2) References (o), (p), and (q) regarding IA and protection.

(3) References (r) and (s) regarding interoperability and NR KPP requirements.

(4) Volumes 1 through 4 of Reference (t), regarding classified and controlled unclassified information.

(5) DoDD 5400.11 (Reference (w)) and DoD 5400.11-R (Reference (x)) regarding requirements of the DoD Privacy Program.

3. DEPUTY CHIEF MANAGEMENT OFFICER OF THE DEPARTMENT OF DEFENSE (DCMO). In addition to the responsibilities in section 8 of this enclosure, the DCMO:

a. In coordination with the USD(P&R), ensures that GFM DI org server enterprise force structure data requirements are sufficiently represented in the defense business enterprise architecture to effectively guide, constrain, and permit implementation of enterprise force structure representation and hierarchy.

b. As provided by section 2222 of Title 10, United States Code (Reference (yx)), ensures the investment review process considers withholding certification of funds as an appropriate control criterion for any appropriate defense business system that fails to meet the defense business enterprise architecture requirements for enterprise force structure or lacks a plan to comply with enterprise force structure requirements within the business enterprise architecture.

4. UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS- SUSTAINMENT (USD(AT&L-A&S)). In addition to the responsibilities in section 8 of this enclosure, the USD(AT&L-A&S):

a. In coordination with the USD(P&R) and the Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense, validates that enterprise force structure data pursuant to this instruction is used in DoD IT systems to the lowest tactical level technically feasible for any DoD force structure representation applicable to that system.

b. As the lead agent for DoD-wide unique identification pursuant to Reference (f), establishes and maintains the policy and standards for the authoritative linkage in IT systems that consume org server data of OUIDs with the other unique identifiers mandated by Reference (f), to include:

(1) Unique identifiers for tangible property, described in DoDI 8320.04 (Reference (z));

(2) Unique identifiers for real property, described in DoDI 4165.14 (Reference (aa)).

c. Provides representation to GFM DI governance bodies.

5. USD(I). In addition to the responsibilities in section 8 of this enclosure, the USD(I):

a. Develops supporting guidance, as necessary, for implementation of this instruction.

b. Provides representation to GFM DI governance bodies.

c. Validates GFM DI policy and artifacts in collaboration with the CJCS and the OSD and DoD Component heads.

d. Pursuant to the procedures detailed in Enclosure 3 of this instruction:

(1) Populates and maintains a SIPRNET-based Defense Intelligence Org Server (DIOS) that documents the relatively permanent structure of:

(a) The Defense Intelligence Agency (DIA)

(b) The National Reconnaissance Office (NRO)

(c) The National Geospatial-Intelligence Agency (NGA)

(d) The National Security Agency (NSA)

(2) Coordinates with USD(P&R) to document within the OSDOS all other organizations over which the USD(I) exercises the Secretary of Defense's authority, direction, and control pursuant to DoDD 5143.01 (Reference (ab)).

(3) Manages investments for DIOS development and maintenance pursuant to Reference (j).

(4) Publishes the pedigree, security level, and access control level of DIOS data through the applicable registries pursuant to Reference (k).

(5) Provides DIOS functionality pursuant to GFM DI technical guidance, including References (l), (m), and (n).

(6) Exposes DIOS data to external consumer systems in compliance with:

(a) References (d), (e), (f), and (g) regarding sharing and management of enterprise information.

(b) References (o), (p), and (q) regarding IA and protection.

(c) References (r) and (s) regarding interoperability and NR KPP requirements.

(d) Volumes 1 through 4 of Reference (t) regarding classified and controlled unclassified information.

(7) Coordinates with USD(P&R) to publish, within the file of reference data common to all DoD Components, that reference data specific to the NRO and the Defense Intelligence combat support agencies (CSAs) for use in systems that involve billets from those organizations.

(8) Documents and manages joint billets and joint billet OUIDs pursuant to Reference (l) and paragraph 2d(3) of Enclosure 3 of this instruction.

(9) In coordination with the DoD CIO and USD(P&R), fully supports the transition to a force management process that enables the global sourcing of operational needs, pursuant to References (c), (u), and (v).

6. DoD CIO. In addition to the responsibilities in section 8 of this enclosure, the DoD CIO:

a. Coordinates with the OSD and DoD Component heads to implement this instruction and establish policies that support the use of enterprise force structure across DoD IT systems to the lowest tactical level technically feasible for any DoD force structure representation applicable to those system with minimal data mediation needs.

b. Monitors compliance with standards for developing, maintaining, and implementing sound, integrated, interoperable, and secure architectures across the DoD, including intelligence systems and architectures, pursuant to References (o) through (s).

7. DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA). Under the authority, direction, and control of the DoD CIO and in addition to the responsibilities in section 8 of this enclosure, the Director, DISA:

a. Develops, integrates, operates, and sustains net-centric enterprise services (NCES) that provide:

(1) A data publication and subscription capability on both the NIPRNET and SIPRNET.

(2) A cross domain capability to synchronize unclassified data between the NIPRNET and SIPRNET security domains.

b. Provides guidance and sets standards for development and implementation of enterprise service-related tools, repositories, and infrastructure for the DoD.

c. Provides services and capabilities that are operated and maintained at levels that meet the operational readiness and warfighting requirements of the Combatant Commanders (CCDRs), in accordance with DoDD 5105.19 (Reference (ac)).

8. OSD AND DoD COMPONENT HEADS. OSD and DoD Component heads:

a. Implement this instruction effectively in their respective areas of responsibility, pursuant to the procedures detailed in Enclosure 3 of this instruction.

b. Integrate enterprise force structure data for any force structure representation applicable to IT systems under their purview, including institutional manpower, personnel, and resource systems, to the lowest tactical level technically feasible, and the maximum extent allowed by law and DoD policy.

c. Pursuant to section 2 of this enclosure, establish and maintain authoritative linkages between billet-level enterprise force structure unique identifiers under their purview and the EDI-PI of the individuals serving in those billets. In coordination with *Director*, DoDHRA through *Director*, DMDC, publish those linkages to an enterprise repository.

9. SECRETARIES OF THE MILITARY DEPARTMENTS. In addition to the responsibilities in section 8 of this enclosure, the Secretaries of the Military Departments:

a. Develop supporting guidance, as necessary, for implementation of this instruction.

b. Provide representation to GFM DI governance bodies.

c. Validate GFM DI policy and artifacts in collaboration with the CJCS and the OSD and DoD Component heads.

d. Pursuant to the procedures detailed in Enclosure 3 of this instruction:

(1) Populate and maintain NIPRNET and SIPRNET org servers that document the relatively permanent placement of all force structure for their respective Military Services, both authorized forces in the administrative chain of command, and the assignment of forces to the operational command structure of the CCMDs:

(a) Air Force Org Server (AFOS)

(b) Army Org Server (AOS)

(c) Marine Corps Org Server (MCOS)

(d) Navy Org Server (NOS)

(2) Replicate in a SIPRNET Military Service org server all data in the applicable NIPRNET org server for augmentation with classified data.

(3) Manage investments for Military Service org server development and maintenance pursuant to Reference (j).

(4) Publish the pedigree, security level, and access control level of Military Service org server data through the applicable registries pursuant to Reference (k).

(5) Provide Military Service org server functionality pursuant to GFM DI technical guidance, including References (l), (m), and (n).

(6) Expose Military Service org server data to external consumer systems in compliance with:

(a) References (d), (e), (f), and (g) regarding sharing and management of enterprise information.

(b) References (o), (p), and (q) regarding IA and protection.

(c) References (r) and (s) regarding interoperability and NR KPP requirements.

(d) Volumes 1 through 4 of Reference (t) regarding classified and controlled unclassified information.

(7) Publish, from both the NIPRNET and SIPRNET org server of the respective Military Service, the file of Military Service-specific reference data for use by data consumers, including other org servers, which involve joint billets.

(8) Document and manage joint billets and joint billet OUIDs pursuant to Reference (l) and paragraph 2d(3) of Enclosure 3 of this instruction.

(9) In coordination with OSD, CJCS, the other Secretaries of the Military Departments, and the CCDRs, fully support the transition to a force management process that enables the global sourcing of operational needs, pursuant to References (c), (u), and (v).

10. CJCS. In addition to the responsibilities in section 8 of this enclosure, the CJCS:

a. Centrally manages the implementation of the GFM DI via the Joint Staff Force Structure, Resources, and Assessment Directorate (J-8).

(1) Establishes functional requirements and responsibilities for the electronic documentation in org servers of the relatively permanent placement of forces in both the administrative chain of command and the operational chain of command, down to the billet level in compliance with Reference (m).

(2) Establishes functional requirements and responsibilities for consumers of org server data regarding the electronic documentation of the relatively temporary placement of attached forces under operational control, tactical control, direct support, and general support relationships between organizational elements of DoD force structure, including ad hoc task organizations, down to the billet level in compliance with Reference (m).

b. Develops supporting guidance and assists the USD(P&R) in resolving disagreements, as necessary, for implementation of this instruction.

c. Pursuant to the procedures detailed in Enclosure 3 of this instruction:

(1) Populates and maintains a Joint Org Server (JOS) that documents the relatively permanent placement of all force structure within the Joint Staff, CJCS-controlled activities, the headquarters of the CCMDs, National Guard Bureau (NGB), and the U.S. elements of North Atlantic Treaty Organization (NATO) and North American Aerospace Defense Command (NORAD).

(2) Replicates in the SIPRNET JOS all data in the NIPRNET JOS for augmentation with classified data. Both the NIPRNET and SIPRNET JOS must contain the necessary linkages to account for joint personnel and equipment authorizations.

(3) Manages investments for JOS development and maintenance pursuant to Reference (j).

(4) Publishes the pedigree, security level, and access control level of JOS through the applicable registries pursuant to Reference (k).

(5) Provides JOS functionality pursuant to GFM DI technical guidance, including References (l), (m), and (n).

(6) Exposes JOS data to external consumer systems in compliance with:

(a) References (d), (e), (f), and (g) regarding sharing and management of enterprise information.

(b) References (o), (p), and (q) regarding IA and protection.

(c) References (r) and (s) regarding interoperability and NR KPP requirements.

(d) Volumes 1 through 4 of Reference (t) regarding classified and controlled unclassified information.

(7) Publishes, from both the NIPRNET and SIPRNET JOS, the file of reference data specific to the Joint Staff, headquarters of the CCMDs, and the NGB, for use by data consumers, including other org servers, that involve joint billets.

(8) Documents and manages joint billets and joint billet OUIDs pursuant to Reference (l) and paragraph 2d(3) of Enclosure 3 of this instruction.

(9) In coordination with OSD, the Secretaries of the Military Departments, and the CCDRs, fully supports the transition to a force management process that enables the global sourcing of operational needs, pursuant to References (c), (u), and (v).

11. CCDRs. In addition to the responsibilities in section 8 of this enclosure, the CCDRs:

a. Implement this instruction effectively in their respective areas of responsibility.

b. Support data population and management of the JOS by documenting the enterprise force structure of CCMD headquarters in compliance with GFM DI technical standards and data implementation business rules approved as configuration control items (see paragraph 1a(2) of Enclosure 3 of this instruction), and other applicable guidance.

c. In coordination with OSD, the CJCS, and the Secretaries of the Military Departments, fully support the transition to a force management process that enables the global sourcing of operational needs, pursuant to References (c), (u), and (v).

12. CHIEF, NGB. In addition to the responsibilities in section 8 of this enclosure, the Chief, NGB:

a. Implements this instruction effectively in his or her respective areas of responsibility.

b. Supports data population and management of the JOS by documenting the enterprise force structure of NGB headquarters in compliance with GFM DI technical standards and data implementation business rules approved as configuration control items (see paragraph 1a(2) of Enclosure 3 of this instruction), and other applicable guidance.

c. In coordination with OSD, the CJCS, and the Secretaries of the Military Departments, fully supports the transition to a force management process that enables the global sourcing of operational needs, pursuant to References (c), (u), and (v).

ENCLOSURE 3

PROCEDURES

1. GFM DI GOVERNANCE

a. The GFM DI is centrally managed by the Joint Staff J-8 and is guided by a collaborative OSD, Joint Staff, Military Service, and interagency COI that utilizes governance and technical bodies to facilitate the development and implementation of objectives. The GFM DI governance structure, to include the various governance and technical bodies, established in accordance with DoDI 5105.18 (Reference (ad)) must consist of full-time or permanent part-time federal officers or employees. Subject matter experts (SMEs), who are not full-time or permanent part-time federal officers or employees, may provide SME advice to the GFM DI governance structure. However, such individuals are prohibited from participating in the governance structure's deliberation process.

(1) Senior level oversight for GFM DI processes is provided by a General Officer Steering Committee (GOSC), chaired by a J-8 representative.

(2) Approval and configuration control of GFM DI technical artifacts is administered by the GFM DI Configuration Control Board (CCB), for which the configuration management authority is the GFM DI GOSC Chair.

b. The initiative is executed in a decentralized manner by the DoD Components, who provide:

(1) Senior representatives to the GOSC.

(2) Policy and technical experts to the CCB and working groups that meet periodically or in special sessions.

2. ORG SERVER PROCEDURES AND REQUIREMENTS

a. The enterprise force structure of the U.S. military is divided into two branches of the chain of command, as described in section 4 of chapter 2 of Joint Publication 1 (Reference (ae)). The authoritative baselines of these branches are comprised of the relatively permanent placement of forces and organizations into command structure hierarchies in accordance with Service doctrine, Reference (u), and Reference (v). These baselines for the administrative command structure and operational command structure are digitally populated within suites of org servers by force management experts of the DoD Components, as identified in Enclosure 2 of this instruction, in accordance with the configuration control items approved by the GFM DI CCB (including References (l), (m), and (n)).

b. The org servers are net-centric services that reside in security domains commensurate with the data they produce. The org servers provide access to organizational data that conforms to the representational precepts of the Organizational and Force Structure Construct (OFSC), pursuant to Reference (m). In accordance with Reference (l), all org server data must be originally created in the security domain commensurate with its classification, and all attributes assigned to that data must share that classification, including their unique identification tags as described in paragraph 2c of this enclosure.

(1) The unclassified enterprise force structure baseline, founded on congressional authorizations for procurement and as organized by the DoD Components, is populated across a suite of org servers on the NIPRNET. As shown in the table, unclassified org servers must be established and maintained by the Military Services, the CJCS, and the USD(P&R).

Table. The Component Org Servers

Name (Acronym)	Security Domain	Enterprise Force Structure Hierarchy	Responsible Office
Air Force Org Server (AFOS)	NIPRNET and SIPRNET	United States Air Force (Active and Reserve Components, and embedded government civilians, and embedded contractors)	Secretary of the Air Force
Army Org Server (AOS)	NIPRNET and SIPRNET	United States Army (Active and Reserve Components, and embedded government civilians, and embedded contractors)	Secretary of the Army
Defense Intelligence Org Server (DIOS)	SIPRNET ONLY	DIA, NGA, NRO, and NSA	USD(I)
Joint Org Server (JOS)	NIPRNET and SIPRNET	Joint Staff, CJCS-controlled activities, the headquarters of the CCMDs, NGB, and the U.S. elements of NATO and NORAD.	CJCS
Marine Corps Org Server (MCOS)	NIPRNET and SIPRNET	United States Marine Corp (Active and Reserve Components, and embedded government civilians, and embedded contractors)	Secretary of the Navy
Navy Org Server (NOS)	NIPRNET and SIPRNET	United States Navy (Active and Reserve Components, and embedded government civilians, and embedded contractors)	Secretary of the Navy
OSD Org Server (OSDOS)	NIPRNET and SIPRNET	OSD Components and the Defense Agencies and DoD Field Activities that report to them, except the four Intelligence Agencies under purview of the DIOS	USD(P&R)

(2) The unclassified baselines are mirrored in a companion suite of org servers that incorporate classified command structure. Classified org servers are to be established and maintained by the Military Services, the CJCS, the USD(P&R), and the USD(I). As shown in the table, the DIOS exists only on the SIPRNET.

c. In accordance with Reference (l), all data within the org servers must be uniquely identified with a global force management identifier (GFMID) and its OUID subset for

organizational elements. The OUID implements the requirement for unique identification for organizations as directed by Reference (f).

d. In accordance with the OFSC detailed in Reference (m), the enterprise force structure baselines documented in the org servers must include all organizational elements in their hierarchal positions of relative permanence.

(1) All DoD doctrinal organizations, both predominately military (Active and Reserve Components) and civilian (OSD, Defense Agencies, and DoD Field Activities), organized into hierarchies in accordance with Military Service, joint doctrine, and OSD policy.

(2) All DoD crew organizations that correspond to platforms that transport their operator(s).

(3) All DoD billet-level organizational elements, including the Military Service members as well as civilians ~~and contractors~~ included in authoritative manning documents. In accordance with Reference (1), billet OUIDs are documented and managed by the component that is the authoritative manager or processor of the majority of that billet's activity.

(a) The JOS is the authoritative data source for the OUIDs of Military Service billets under CJCS authority, as well as Combatant Command Headquarters Staff, NGB authority, and the U.S. elements of NATO and NORAD.

(b) The OSDOS is the authoritative data source for the OUIDs of Military Service billets under the authority of the OSD Components or the organizations that report to them (i.e., the Defense Agencies or Field Activities), except for those Defense Intelligence organizations in the DIOS.

(c) The DIOS is the authoritative data source for the OUIDs of Military Service billets within the NRO and the three Defense Intelligence CSAs.

(d) For the OUIDs of joint billets in Military Service organizations, the org server of the Military Service that manages or processes the majority of that billet's activity (i.e., the Military Service to which the billet is embedded and performs the majority of its duties) is the authoritative source. Instances in which the determination of a billet's majority activity is unclear are to be adjudicated by the Military Services involved.

e. In accordance with Reference (n) and guidance of the CCB, the enterprise force structure baselines documented in the org servers must also include the authorization inventory for all DoD crewed platforms and beyond line-of-sight unmanned aerial vehicles.

f. Every org server must publish, in compliance with GFM DI artifacts and tagged with authoritative GFMIDs, the file of official reference data unique to that Component, for use by other org servers and consumers of org server data. Reference data includes person-types, person-type skill attributes, alias-types, and materiel-types. USD(P&R) must publish the file of

DoD-wide reference data which is used across DoD Components (see section 1d(7)(a) of Enclosure 2 of this instruction).

g. In accordance with paragraph 1d(7)(c) of Enclosure 2 of this instruction, USD(P&R) must also be responsible for publishing the upper echelon force structure data common to all of the DoD Components, known as the Bridge and as described in section 18 of Reference (m).

h. In accordance with Reference (n), the org servers must include equipment-type data associated with crew organizations. Equipment authorized to billet organizations (i.e., necessary to fulfill the billet's function), may also be associated but are not mandated.

i. In accordance with Reference (n), the org servers must include the enterprise force structure baselines for the current year as well those programmed over the 6 future years of the Future Years Defense Program database. As historical data accumulates, it is to be preserved in perpetuity, with 6 previous years' data resident within the org servers, and data beyond 6 years archived externally and available to authorized users.

j. In accordance with References (e) and (n), org servers are to provide data that is timely, reliable, and accurate.

k. In accordance with References (e) and (f), org server data is a strategic asset that must be appropriately secured, shared, and made available to any DoD user or mission partner to the maximum extent allowed by law and DoD policy. Data is to be made available via the publication and subscription capabilities provided by the NCES of the DoD Information Network (DoDIN).

l. The org servers provide baselines only for enterprise force structure in positions of relative permanence, both for authorized forces within the administrative command structure and assigned forces within the CCMDs. Temporary changes to those baselines (e.g., attached forces) are documented by external consumers of enterprise force structure data.

(1) Systems across the DoD must consume, integrate, and augment enterprise force structure data in order to document allocated forces, and any other task organization under operational control, tactical control, support relationships, or temporary changes in administrative control, to provide the basis for integration of timely real world data (e.g., readiness, current location, planning and execution, logistics, and personnel data).

(2) Enterprise force structure data may be either consumed directly from the org servers or indirectly from intermediary systems.

m. To enable DoD-wide interoperability, all DoD IT systems that document force structure related information must represent and identify such force structure in accordance with this instruction. The common format of enterprise force structure is to be implemented natively by consumer systems, or else mediated by service-oriented architecture applications to support consumption for local use and translation back into the common format for exposure to the

DoDIN. Consumer systems that expose integrated or augmented force structure data to the DoDIN must do so in compliance with:

- (1) References (d), (e), (f), and (g) regarding sharing and management of enterprise information.
 - (2) References (o), (p), and (q) regarding IA and protection.
 - (3) References (r) and (s) regarding interoperability and NR KPP requirements.
 - (4) Volumes 1 through 4 of Reference (t), regarding protection of classified and controlled unclassified information.
 - (5) References (w) and (x) regarding requirements of the DoD Privacy Program.
- n. Future and legacy systems need to consume enterprise force structure, in whole or in part.
- (1) For legacy systems, OUID integration alone may satisfy the data-sharing goals of Reference (e).
 - (2) Due to technical constraints of the tactical environment, tactical edge emitters such as military force tracking systems must integrate their identifiers with OUIDs at the lowest echelon that is technically feasible (e.g., operation centers) for dissemination back through the tactical net.
- o. Investments for org server development and maintenance, and for the consumption of org server data by consumer systems, are to be managed in accordance with Reference (l).

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

AFOS	Air Force Org Server
AOS	Army Org Server
ASD	Assistant Secretaries of Defense
ATSD	Assistants to the Secretary of Defense
CCB	Configuration Control Board
CCDR	Commander of a Combatant Command
CCMD	Combatant Command
CJCS	Chairman of the Joint Chiefs of Staff
COI	community of interest
CSA	combat support agency
D CMO	D eputy Chief Management Officer of the Department of Defense
DIA	Defense Intelligence Agency
DIOS	Defense Intelligence Org Server
DISA	Defense Information Systems Agency
DMDC	Defense Manpower Data Center
DoD CIO	DoD Chief Information Officer
DoDD	DoD directive
DoDHRA	DoD Human Resources Activity
DoDI	DoD instruction
DoDIN	DoD Information Network
EDI-PI	electronic data exchange personal identifier
GC DoD	General Counsel of the Department of Defense
GFMID	global force management identifier
GFM DI	Global Force Management Data Initiative
GOSC	General Officer Steering Committee
IA	information assurance
IG DoD	Inspector General of the Department of Defense

IT	information technology
J-8	Joint Staff Force Structure, Resources, and Assessment Directorate
JOS	Joint Org Server
MCOS	Marine Corps Org Server
NATO	North Atlantic Treaty Organization
NOS	Navy Org Server
NCES	net-centric enterprise services
NGA	National Geospatial-Intelligence Agency
NGB	National Guard Bureau
NIPRNET	Non-Secure Internet Protocol Router Network
NORAD	North American Aerospace Defense Command
NR KPP	Net Ready Key Performance Parameter
NRO	National Reconnaissance Office
NSA	National Security Agency
OFSC	Organizational and Force Structure Construct
OSDOS	OSD Org Server
OID	organization unique identifier
PSA	Principal Staff Assistant
SIPRNET	SECRET Internet Protocol Router Network
SME	subject matter expert
USD(AT&L A&S)	Under Secretary of Defense for Acquisition, Technology, and Logistics Sustainment
USD(I)	Under Secretary of Defense for Intelligence
USD(P&R)	Under Secretary of Defense for Personnel and Readiness

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purposes of this instruction.

administrative chain of command. One of the two branches of the chain of command described in Reference (ae), through which command is exercised from the President through the Secretary of Defense to the Secretaries of the Military Departments, and from which forces are assigned to CCMDs to compose the operational command structure baseline. ~~This term and its definition are proposed for inclusion in the next edition of Joint Publication 1-02 DoD Dictionary of Military and Associated Terms (Reference (af)).~~

administrative command structure. The organizational hierarchy through which administrative leadership is exercised, as contrasted by the operational command structure through which operational authority is exercised. ~~This term and its definition are proposed for inclusion in the next edition of Reference (af).~~

administrative leadership. The authorities exercised over subordinates by virtue of rank or assignment in the administrative chain of command, for the accomplishment of administrative functions prescribed pursuant to Reference (y).

allocated forces. Defined in Reference (v).

assigned forces. Defined in Reference (v).

assignment. Defined in Reference (v).

attached forces. Defined in Reference (v).

authorization data. DoD military and civilian manpower and equipment resources authorized by law. ~~This term and its definition are proposed for inclusion in the next edition of Reference (af).~~

authorization inventory. The set of manpower and equipment authorizations associated with one or more organization. ~~This term and its definition are proposed for inclusion in the next edition of Reference (af).~~

billet organization. Defined in Reference (m).

chain of command. Defined in Reference (af).

COI. Defined in Committee on National Security Systems Instruction 4009 (Reference (ae)).

command structure. The organizational hierarchy through which administrative leadership or operational authority is exercised. ~~This term and its definition are proposed for inclusion in the next edition of Reference (af).~~

crew organization. Defined in Reference (m).

crewed platform. Used in accordance with the definitions for crew organization and platform in Reference (m).

defense business enterprise architecture. Defined in section 2222c of Reference (y).

doctrinal organization. Defined in Reference (m).

EDI-PI. As described in the text of DoDI 1000.30 (Reference (ah)), the EDI-PI is a unique personal identifier created within the Defense Enrollment Eligibility Reporting System for each person who has a direct relationship with the DoD. The DoD identification number is the common name for the EDI-PI.

enterprise. Defined in Reference (f).

enterprise force structure. The digitized hierarchical representation of DoD organizations, documented in accordance with the standardized precepts of the OFSC, generated and shared from org servers for DoD-wide integration and use. ~~This term and its definition are proposed for inclusion in the next edition of Reference (af).~~

force management. An organizing construct of processes, policies, organizational information, and tools that informs senior leader decision making on the global joint sourcing of the defense strategy. ~~This term and its definition are proposed for inclusion in the next edition of Reference (af).~~

force structure. The composition of DoD organizations, both military and civilian, that comprise and support U.S. defense forces as specified by the National Defense Authorization Acts of current and applicable previous years, and defines the organizational hierarchy through which leadership authorities are exercised. ~~This term and its definition are proposed for inclusion in the next edition of Reference (af).~~

GFM DI. Defined in Reference (m).

GF MID. An alias for the Global Force Management Identifier defined in Reference (l), used to distinguish it from the Force Module Identifier used by the Joint Operational Planning and Execution System.

global force management. A process to align assignment, allocation, and apportionment of forces to CCDRs in support of the National Defense Strategy and joint force availability requirements. ~~This term and its definition are proposed for inclusion in the next edition of Reference (af).~~

information life cycle. Defined in Reference (d).

IT. Defined in Reference (r).

OFSC. The standardized precepts for the digitization of hierarchical enterprise force structure data for DoD-wide integration and use. ~~This term and its definition are proposed for inclusion in the next edition of Reference (af).~~

operational chain of command. One of the two branches of the chain of command described in Reference (ae), through which command is exercised from the President through the Secretary of Defense to the CCDRs, to whom forces are assigned and allocated via the global force management process. ~~This term and its definition are proposed for inclusion in the next edition of Reference (af).~~

operational command structure. The organizational hierarchy through which operational authorities are exercised, as contrasted by the administrative command structure through which administrative leadership is exercised. ~~This term and its definition are proposed for inclusion in the next edition of Reference (af).~~

organizational (org) server. Defined in Reference (m).

organizational element. Defined in Reference (m).

OSD. In accordance with DoDD 5100.01 (Reference (ai)), OSD comprises the Deputy Secretary of Defense, who also serves as the Chief Management Officer of the Department of Defense; the Under Secretaries of Defense; the ~~D~~CMO; the General Counsel of the Department of Defense (GC DoD); the Assistant Secretaries of Defense (ASDs); the Assistants to the Secretary of Defense (ATSDs); the OSD Directors, and equivalents, who report directly to the Secretary or the Deputy Secretary of Defense; their staffs; the IG DoD; and such other staff offices within OSD established by law or the Secretary of Defense to assist in carrying out assigned responsibilities.

OSD Component. An OSD office led by a Principal Staff Assistant (PSA). As described in the text of Reference (ai), the PSAs thus constitute the “Heads of the OSD Components.” OSD organizations subordinate to an OSD Component are not themselves OSD Components. Defense Agencies and DoD Field Activities are established by law as DoD Components and are thus neither OSD Components nor a part of OSD, although all are currently under the authority, direction, and control of the OSD Component PSAs.

organization. Defined in Reference (m).

organizational element. Defined in Reference (m).

platform. Defined in Reference (m).

PSA. As described in the text of Reference (ai), the Under Secretaries of Defense; the ~~D~~CMO; the GC DoD; the IG DoD; and those ASAs, ATSDs, and OSD Directors, and equivalents who report directly to the Secretary or Deputy Secretary of Defense.

unit organization. Defined in Reference (m).