Department of Defense
INSTRUCTION

NUMBER 8110.01
November 25, 2014

DoD CIO

SUBJECT: Mission Partner Environment (MPE) Information Sharing Capability Implementation for the DoD

References: See Enclosure 1

1. PURPOSE. This instruction:

a. Reissues DoD Instruction (DoDI) 8110.1 (Reference (a)) in accordance with the authority in DoD Directive (DoDD) 5144.02 (Reference (b)).

b. Establishes policy, assigns responsibilities, and provides procedures for a DoD-wide policy framework for implementation of an MPE capability that responds to major combat operations (MCO), humanitarian and disaster relief operations, defense support of civil authorities (DSCA), and U.S.- and non-U.S.-led cooperative security activities.

2. APPLICABILITY

a. This instruction applies to:

(1) OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this instruction as the "DoD Components").

(2) Any DoD-owned or -managed mission partner (MP) electronic information sharing capabilities used by the DoD Components that exchange information up to and including SECRET.

b. This instruction does **not** apply to programs or systems granted exceptions pursuant to Enclosure 3 of this instruction.

c. Nothing in this instruction alters or supersedes the existing authorities and policies of the Director of National Intelligence regarding all intelligence-related information, as directed by Executive Order (E.O.) 13526 (Reference (c)).

3. POLICY. It is DoD policy that:

a. In order to defend the Nation and enhance global stability in accordance with References (c) through (g), the DoD will, in accordance with DoDI 5200.01 and Volumes 1 through 4 of DoD Manual 5200.01 (References (h) and (i)), promote effective information exchange among the MPs, which include:

(1) Other federal, State, local, and tribal agencies.

(2) Allies, coalition members, host nations, and other nations.

(3) U.S. and international non-governmental organizations.

(4) Multinational treaty organizations.

(5) Private sector organizations.

b. DoD information will be visible, accessible, understandable, trustworthy, secure, interoperable, and made available to appropriate MPs, to the maximum extent allowed by law or DoD policy.

(1) All electronic data and information collected, maintained, used, or shared will adhere to the requirements and restrictions imposed by section 552a of Title 5, United States Code (U.S.C.) (Reference (j)), DoDDs 5400.11 and 5240.01, and DoDI 1000.29 (References (k), (l), and (m)); and other federal laws, E.O.s, and DoD policies regarding the protection of privacy information and civil liberties.

(2) Special emphasis will be placed on protecting information pertaining to U.S. citizens in accordance with DoD 5400.11-R (Reference (n)) and section 803 of Public Law 110-53 (Reference (o)).

c. A common set of standards, protocols, and interfaces will be used to enable the sharing of DoD data, information, and information technology (IT) services pursuant to References (n), (o), and DoDI 8551.01 (Reference (p)). The National Information Exchange Model (NIEM), in accordance with the DoD Data Framework as addressed by the National Strategy for Information Sharing and Safeguarding Memorandum (Reference (q)) and as described in DoD Chief Information Officer (DoD CIO) Memorandum (Reference (r)), is the first point of reference when deciding which data exchange standards or specifications meet mission and operational needs. To the maximum extent possible, the DoD's common information sharing standards, protocols, and interfaces will be compatible and interoperable with those of other federal departments, agencies, and MPs.

d. The DoD will use a comprehensive, widely understood information sharing governance framework for creating and sustaining a federated information sharing community of organizations and individuals pursuant to the Assistant Secretary of Defense for Networks and Information Integration/DoD CIO Memorandum (Reference (d)).

e. The DoD will improve electronic MPE information sharing capability in accordance with the Quadrennial Defense Review Report (Reference (s)).

f. The MPE will adhere to the priorities outlined in the Future Mission Network (FMN) 90 Day Study Report as validated in the Joint Requirements Oversight Council Memorandum (JROCM) 026-13 (Reference (t)) and the Joint Staff Directorate for Command, Control, Communications, and Computers (J-6) Report(Reference (u)).

g. The MPE will synchronize with the Deputy Secretary of Defense Memorandum (Reference (v)) and the Joint Staff J-6 Initial Capabilities Document (ICD) for Joint Information Environment (JIE) (Reference (w)) and Defense Intelligence Information Environment (DI2E) concepts to achieve mission success in a secure, efficient, and cost effective manner.

h. Authorization for disclosure and handling of classified, controlled unclassified information, unclassified information, and data shared with MPs will be determined in accordance with U.S. law and DoD policies and guidance to include E.O. 13526 (Reference (e)), References (h) and (i), E.O. 12333 (Reference (x)), DoDD 5230.11 (Reference (y)), and DoDI 2040.02 (Reference (z)).

i. The MPE will serve as the framework for operational information sharing between DoD Components and MPs.

j. A mission-based interoperability compliance and assessment enduring capability will be sustained and utilized to support MPE.

4. RESPONSIBILITES. See Enclosure 2.

5. PROCEDURES. See Enclosure 3.

6. RELEASABILITY. **Cleared for public release**. This instruction is available on the Internet from the DoD Issuances Website at http://www.dtic.mil/whs/directives.

7. EFFECTIVE DATE. This instruction is effective November 25, 2014.

Terry A. Halvorsen
Acting Department of Defense
Chief Information Officer

Enclosures
1. References
2. Responsibilities
3. Procedures

Glossary

TABLE OF CONTENTS

ENCLOSURE 1

REFERENCES

(a) DoD Instruction 8110.1, "Multinational Information Sharing Networks Implementation," February 6, 2004 (hereby cancelled)
(b) DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014
(c) Executive Order 13526, "Classified National Security Information," December 29, 2009
(d) Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, "DoD Information Sharing Strategy," May 4, 2007
(e) Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," February 19, 2013
(f) DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise," February 10, 2009
(g) Presidential Policy Directive-21, "Critical Infrastructure Security and Resilience," February 12, 2013
(h) DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information," October 9, 2008, as amended
(i) DoD Manual 5200.01, Volumes 1-4, "DoD Information Security Program," February 24, 2012, as amended
(j) Section 552a of Title 5, United States Code (also known as "The Privacy Act of 1974"), as amended
(k) DoD Directive 5400.11, "DoD Privacy Program," October 29, 2014
(l) DoD Directive 5240.01, "DoD Intelligence Activities," August 27, 2007, as amended
(m) DoD Instruction 1000.29, "DoD Civil Liberties Program," May 17, 2012
(n) DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
(o) Section 803 of Public Law 110-53, "Implementing Recommendations of the 9/11 Commission Act of 2007," August 3, 2007
(p) DoD Instruction 8551.01, "Ports, Protocols, and Services Management (PPSM)," August 28, 2014
(q) Presidential Memorandum, "National Strategy for Information Sharing and Safeguarding," December 2012
(r) DoD Chief Information Officer Memorandum "Adoption of the National Information Exchange Model within the DoD," March 28, 2013
(s) Office of the Secretary of Defense Report, "Quadrennial Defense Review Report," February 20, 2010
(t) Joint Requirements Oversight Council Memorandum 026-13, "Future Mission Network 90 Day Study Report," February 5, 2013
(u) Joint Staff Directorate for Command, Control, Communications, and Computers (J-6), "Future Mission Network 90 Day Study Report," December 17, 2012
(v) Deputy Secretary of Defense Memorandum, "Joint Information Environment Implementation," May 6, 2013
(w) Joint Staff Directorate for Command, Control, Communications and Computers (J-6), Joint Capabilities Integration and Development System, "Initial Capabilities Document (ICD) for The Joint Information Environment (JIE)," June 27, 2012

(x) Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended
(y) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992
(z) DoD Instruction 2040.02, "International Transfers of Technology, Articles, and Services," March 27, 2014
(aa) Section 2223 of Title 10, United States Code
(ab) DoD Instruction 8330.01, "Interoperability of Information Technology (IT), Including National Security Systems (NSS)," May 21, 2014
(ac) Department of Defense Chief Information Officer Memorandum, "Interim Guidance for Interoperability of Information Technology (IT) and National Security Systems (NSS)," March 27, 2012
(ad) Chairman of the Joint Chiefs of Staff Instruction 6285.01C, "Multinational and Other Mission Partner (MNMP) Information Sharing Requirements Management Process," May 15, 2013
(ae) DoD 5400.7-R, "DoD Freedom of Information Act Program," September 4, 1998, as amended
(af) Information Sharing Council, ISC – ISE Guidance, "Information Sharing Environment Guidance (ISE-G) 108", "Identity and Access Management Framework for the ISE version 1.0," December 19, 2008
(ag) Presidential Memorandum, "Guidelines and Requirements in Support of the Information Sharing Environment," December 16, 2005
(ah) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014
(ai) DoD Instruction 8510.01, " Risk Management Framework (RFM) for DoD Information Technology (IT)," March 12, 2014
(aj) Committee on National Security Systems Policy No. 6, "National Policy on Certification and Accreditation of National Security Systems," October 2005
(ak) Committee on National Security Systems Instruction 1253, "Security Categorization and Control Selection for National Security Systems," October 2009
(al) DoD Directive 5015.2, "DoD Records Management Program," March 6, 2000
(am) DoD Principal Accrediting Authorities Memorandum, "DoD Information System Certification and Accreditation Reciprocity," July 23, 2009
(an) DoD Instruction 8220.02, "Information and Communications Technology (ICT) Capabilities for Support of Stabilization and Reconstruction, Disaster Relief, and Humanitarian and Civic Assistance Operations," April 30, 2009
(ao) DoD Instruction 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling," May 24, 2011
(ap) DoD Instruction 8520.03, "Identity Authentication of Information Systems," May 13, 2011
(aq) Chairman of the Joint Chiefs of Staff Instruction 3170.01H, "Joint Capabilities Integration and Development System," January 10, 2012
(ar) Joint Capabilities Integration and Development System (JCIDS) Manual, "Manual for the Operation of the Joint Capabilities Integration and Development System," January 19, 2012
(as) Joint Requirements Oversight Council Memorandum 081-12, "Future Mission Network Initial Capabilities Document," May 31 2012
(at) Section 798 of Title 18, United States Code
(au) DoD Directive 5105.19, "Defense Information Systems Agency (DISA)," July 25, 2006

(av) Director of National Intelligence, Strategy, "United States Intelligence Community Information Sharing Strategy," February 22, 2008
(aw) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I))," October 24, 2014
(ax) National Disclosure Policy -1, "National Disclosure Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations," October 2, 2000
(ay) National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information Systems," July 5, 1990
(az) DoD Instruction 5025.01, "DoD Issuances Program," June 6, 2014, as amended
(ba) DoD Chief Information Officer Memorandum, "Defense Information Enterprise Architecture (DIEA)," August 10, 2012
(bb) Joint Requirements Oversight Council Memorandum 081012, "Initial Capabilities Document (ICD) For A Future Mission Network (FMN)," May 31, 2012
(bc) Chairman of the Joint Chiefs of Staff Instruction 8501.01B, "Chairman of the Joint Chiefs of Staff; Combatant Commanders; Chief, National Guard Bureau; and Joint Staff Participation in the Planning, Programming, Budgeting and Execution Process," August 21, 2012
(bd) Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," current version

ENCLOSURE 2

RESPONSIBILITIES

1. DoD CIO. The DoD CIO:

a. Monitors, evaluates, and provides advice on the interoperability, performance, and functionality of electronic MPE information sharing capability to the Secretary and Deputy Secretary of Defense and the OSD Component heads in accordance with References (c) and (aa) through (ac).

b. Establishes a centralized MPE governance process to develop policies, issue guidance, and provide strategic vision and oversight of the integration and evolution of MPE capabilities in coordination with the CJCS and other MPE stakeholders.

c. Co-leads, with the CJCS, MPE capability development, evolution, and implementation activities consistent with Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6285.01C (Reference (ad)).

d. Reviews and provides guidance on funding for sustainment and development of electronic MPE information sharing capability throughout the planning, programming, budgeting, and execution process.

e. Oversees and provides guidance and direction to the Defense Information Systems Agency (DISA) in the execution of its responsibilities in accordance with this instruction, including the management of assigned electronic MPE information sharing capability and standards.

f. Issues DoD guidance, consistent with Reference (b), pursuant to Reference (c), and in accordance with References (d), (j), (m), (r), (x) through (ac), DoD 5400.7-R (Reference (ae)), and other DoD guidance as applicable for:

(1) Enterprise services to promote the availability of discoverable information.

(2) Network standards, procedures, and management to improve consistency and interoperability in accordance with References (q), DoDI 8330.01, and DoD CIO Memorandum (References (ab) and (ac)).

(3) The development and use of data tagging and labeling, multi-level security services, virtual private networks (VPNs), and confidentiality mechanisms in coordination with the National Security Agency/Central Security Service (NSA/CSS), the Unified Cross Domain Management Office, and other organizations to promote assured information sharing.

(4) Technical guidance to automate foreign disclosure and handling mechanisms and procedures to reduce delay and increase the effectiveness of information exchange with MPs as

directed in DoDD 8000.01 (Reference (f)) in coordination with the Under Secretary of Defense for Policy (USD(P)).

(5) Implementation of the provisions of Information Sharing Environment Guidance (ISE-G) 108 (Reference (af)) and Presidential Memorandum (Reference (ag)).

g. Oversees integration of electronic MPE information sharing capability into the operation of existing DoD enterprise services and capabilities.

h. Ensures an appropriate official serves as the authorizing official for networks that support MPE information sharing capability and associated standards, as appropriate, in accordance with References (ah) through (am)).

i. Adjudicates DoD Component requests for exception to the use of enterprise services and interface specifications and standards for the exchange of DoD information with MPs.

j. Requests the inclusion in the DoD Information Technology Standards Registry (DISR) of the core set of agreed upon standards for electronic information sharing, including associated applications for unclassified information sharing capability, developed in coordination with the USD(P), the Under Secretary of Defense for Intelligence (USD(I)), and the CJCS, in accordance with Reference (ab) and DoDI 8220.02 (Reference (an)).

k. Oversees identity authentication and access management policies that support secured, available, and accurate MPE electronic information sharing, in accordance with DoDI 8520.02 (Reference (ao)) and DoDI 8520.03 (Reference (ap)) and in coordination with the USD(I), the USD(P), the Under Secretary of Defense for Personnel and Readiness (USD(P&R)), and the Director, DISA.

l. Oversees and coordinates with the Assistant Director of National Intelligence and CIO the activities of the Unified Cross Domain Management Office (UCDMO) (see glossary for definition) in the development of cross-domain enterprise services, standards, and protocols in support of MPE information sharing.

m. Issues a security classification guide regarding MPE (e.g., software, hardware, architectures, configurations) in coordination with the USD(P), the Director DISA, and the USD(I), and consistent with the requirements of the Committee on National Security Systems Instruction 1253 (Reference (ak)).

n. Monitors and evaluates electronic MPE information sharing capability provided to the DoD Components. Confirms controlled unclassified information protection is considered from the operations security perspective.

o. In coordination with the Director, DISA:

(1) Provides standardized guidance of MPE-exchanged data by the IT network during processing, transport, storage, handling, and distribution.

(2) Verifies the management of records is consistent with DoDD 5015.2 (Reference (al)).

(3) Ensures overall classification markings designated by the original classification authority are maintained in accordance with the Committee on National Security Systems Policy 6 (Reference (aj)) and Reference (ak).

(4) Develops standardized guidance for use with other federal agencies regarding tagging, discovery, and access to data in accordance with Reference (ak) and consistent with the overall classification marking of the data and the established access privileges and :need to know" of the individual MP.

p. In coordination with the USD(I) and the CJCS, provides guidance for the interoperability and security test and certification of MPE information sharing capabilities, their interfaces with each other, and their interfaces with U.S. networks, in accordance with References (ah) through (am).

q. Acts as the sole standard exception adjudication authority.

r. Provides oversight of the mission-based interoperability compliance and assessment capability.

s. Establishes records management procedures for protecting, maintaining, and archiving DoD records within the MPE environment in accordance with Reference (al).

t. Distributes the electronic MPE information sharing capability standard that is certified in accordance with Reference (ai).

u. Coordinates with the Joint Chiefs of Staff and the MPE requirements sponsor in accordance with CJCSI 3170.01H and Joint Capabilities Integration and Development System Manual (References (aq) and (ar)) in addressing validated MPE information sharing requirements.

2. DIRECTOR, 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. In coordination with the DoD CIO, the CJCS, and the requirements sponsor designated by the CJCS in accordance with the procedures in References (ad) and (aq), plans, programs, and budgets for MPE capabilities and supporting infrastructure and infrastructure services.

b. Maintains and supports the Multinational Information Sharing (MNIS) office as the management office with cost, schedule, and performance responsibilities and adequate, qualified resources to sustain existing capabilities, including upgrades and enhancements in accordance with Reference (ad), and supports the planning and execution necessary for MPE capabilities, in accordance with Joint Requirements Oversight Council Memorandum 081-12 (Reference (as)).

c. Evolves the existing enterprise services and interface specifications and standards based on the operational needs of the DoD Components synchronized with validated operational and JIE requirements and requests their inclusion in the DISR.

d. Establishes network connection approval and user registration procedures to support the management of MP information sharing communities' operations.

e. Supports the development of a Combatant Commander's mission-based interoperability compliance and assessment support to ensure coalition interoperability in accordance with approved Coalition Mission Threads. Executes DoD CIO-provided guidance for the interoperability and security assessment of MPE information sharing capability, their interfaces with each other, and their interfaces with U.S. networks, in accordance with References (d) and (x) through (ac).

f. Reviews requests submitted by the DoD Component heads and makes recommendations to the DoD CIO regarding exceptions to the use of prescribed MPE interface specifications and standards for the exchange of DoD information with MPs.

g. Develops, coordinates, and issues technical procedures for the DoD Components to follow when managing and using the electronic MPE information sharing capability.

h. Manages cryptographic keying material for DISA managed networks and the supporting VPN infrastructures for electronic MPE information sharing capability.

i. Participates in the development of identity authentication and access management policies that support secured, available, and accurate information sharing with MPs in coordination with the DoD CIO, USD(I), Director, DIA, USD(P), CJCS, USD(P&R), and the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)).

j. Assists the DoD CIO in developing a security classification guide pursuant to Reference (j) that includes security classification guidance for MPE operations.

k. Provides an accessible electronic repository for MP information sharing agreements for military mission planning and execution, DSCA, and foreign stability, security, transition, and reconstruction operations.

l. Ensures no process within the IT networks compromises the classification and markings of underlying information or permits alteration of such markings as established by the original classification authority. Provides an auditable chain of custody for all classified information, and means for establishing the "need to know" by organization and individual within an organization in accordance with Chapter 37 of Title 18, U.S.C. (Reference (at)).

m. In accordance with Reference (ah), develops MPE interface specifications and standards (as detailed in section 2 of Enclosure 3 of this instruction) certified in accordance with the DoD Risk Management Framework.

n. Provides the mission-based interoperability compliance and assessment core component through the Joint Interoperability Test Command (JITC).

o. Manages the day-to-day operations of mission-based interoperability compliance and assessment with operational direction and mission prioritization from the Joint Staff; management of DoD Component participation; and oversight from DoD CIO. As the U.S. mission-based interoperability compliance and assessment national lead, maintains liaison with established MP interoperability, assurance, or validation organizations and activities.

p. In conjunction with the Deputy Assistant Secretary of Defense for Developmental Test and Evaluation (DASD(DT&E)), the Director of Operational Test and Evaluation (DOT&E), and the CJCS, develops a mission-based interoperability test and evaluation methodology for coalition environments to be accomplished in conjunction with the developmental and life-cycle management for programs of record and non-programs of record that support MPE.

q. Updates the DoD CIO annually on overall test and evaluation strategy for certifying MPE interoperability and validating the integration of coalition standards pursuant to requisite DoD authorities as described in Reference (c) and DoDD 5105.19 (Reference (au)).

3. USD(I). The USD(I):

a. Provides direction and guidance, pursuant to the Director of National Intelligence Memorandum (Reference (av)), to the DoD Components for the use of DoD non-compartmented intelligence information, classified up to and including SECRET, hosted on DoD secure networks providing electronic MPE information sharing capability. This direction and guidance will address intelligence information acquisition, analysis processing management, appropriate access to intelligence information, and dissemination considerations.

b. Oversees all DoD intelligence exchange and sharing agreements and supports the CJCS to promote MPE intelligence information sharing capability in accordance with Reference (av) and DoDD 5143.01 (Reference (aw)).

c. Develops, coordinates, and oversees the implementation of DoD policy for sharing intelligence information and interoperability requirements to promote MPE intelligence-sharing capability, in accordance with References (b), (h), (ab), (ac), (aj), and the National Disclosure Policy -1 (Reference (ax)).

d. In coordination with the USD(P), and consistent with References (w) through (ax), develops DoD security plans, policies, and procedures necessary for the effective implementation of foreign disclosure guidance to support MPE intelligence information sharing capability.

e. Serves as the DoD senior security official, pursuant to Reference (ai), to develop and integrate risk-managed security and protection policies and programs that provide MPE intelligence information sharing capability.

f. Provides advice and guidance to the DoD CIO for identity authentication and access management policies that support secured, available, and accurate intelligence information sharing with MPs in coordination with the USD(P), USD(P&R), CJCS, and Director, DISA.

g. Provides advice and guidance to the DoD CIO to develop a security classification guide regarding MPE intelligence information sharing capability pursuant to References (j) and (o).

h. Uses and encourages the use (among defense intelligence and intelligence community (IC) elements) of DISA-developed interface specifications and standards in Defense intelligence systems developed to exchange intelligence information and data, where practical and appropriate. Confirms coordination between DIA and IC systems developers to work with DISA to build an interoperable, enterprise architecture consisting of JIE, DI2E, and IC Information Technology Enterprise frameworks.

4. DIRECTOR, NSA/CHIEF, CSS (DIRNSA/CHCSS). Under the authority, direction, and control of the USD(I), pursuant to National Security Directive 42 (Reference (ay)) and in addition to the responsibilities in section 8 of this enclosure, the DIRNSA/CHCSS:

a. Develops or identifies solutions for secure and dynamic MP information sharing communities and information confidentiality services for the connection of networks that support MPE information sharing capability.

b. Develops or identifies solutions that can be used between or within various network security and information domains.

c. Assists the Director, DISA, in the development or selection of efficient and effective information assurance solutions that will enable secure electronic information sharing, which includes:

(1) Information discovery.

(2) Dynamic MP information sharing communities.

(3) Information privacy services on networks that support MPE electronic information sharing capability.

d. Assists the Director, DISA, in the development of authorization documentation for the solutions recommended by DISA for networks that support MPE electronic information sharing capability in accordance with References (ah) through (ak).

5. USD(P). The USD(P):

a. Approves all proposed policy-significant international agreements before and after any negotiations are concluded, consistent with Reference (z) and Volume 4 of DoDD 5530.3 (Reference (j)).

b. Provides direction and guidance, pursuant to Reference (ax), Reference (r), Reference (z), and Volume 4 of Reference (j), to ensure effective implementation of DoD policy for disclosing classified military information and controlled unclassified information to foreign partners.

c. Coordinates on all DoD classified military information and controlled unclassified information exchange and sharing agreements negotiated and concluded with foreign partners.

d. In coordination with the USD(I) to support information sharing with foreign partners and consistent with Volume 4 of Reference (i), DoDI 5025.01 (Reference az), and References (z), (aa), and (ax), develops DoD plans, policies, and procedures necessary for effective implementation of foreign disclosure guidance for classified and unclassified DoD information throughout the DoD.

e. Oversees, in coordination with the USD(I) and following the guidance provided by Reference (I), the development and distribution of foreign disclosure training requirements throughout DoD to facilitate appropriate information sharing with foreign partners.

6. USD(P&R). In coordination with the DoD CIO, USD(P), USD(I), CJCS, and Director, DISA, the USD(P&R) develops identity authentication and access management policies that support secured, available, and accurate electronic information sharing.

7. USD(AT&L). In coordination with the DoD CIO, the USD(AT&L) determines the appropriate acquisition actions and science and technology developments for electronic MP information sharing capability in accordance with Volume 4 of Reference (i).

8. DoD COMPONENT HEADS. The DoD Component heads:

a. Manage electronic MPE information sharing capability in accordance with applicable statutory, regulatory, DoD acquisition, and security policies and procedures, and following JIE guidelines and priorities as described in Reference (x) and the guidance in Reference (w).

b. Plan, program, and budget for MP-compatible MPE information sharing capability and supporting infrastructure and infrastructure services in coordination with the DoD CIO, the CJCS, and the requirements sponsor designated by the CJCS in accordance with the procedures in References (ad) and (aq). Provide program and budget data to the DoD CIO on an annual or as requested basis.

c. Provide the DoD CIO, through the Director DISA, electronic MPE information sharing program information to ensure DoD Component plans adhere to DoD CIO approved enterprise services, interface specifications, and standards for future MPE information sharing capability.

d. Use existing MPE compatible enterprise services and interface specifications and standards as defined and further developed by DISA for networks that exchange DoD information with MPs up to and including the SECRET classification level, unless an exception is authorized. Requests for exceptions will be coordinated with the Director, DISA, and approved by the DoD CIO in accordance with paragraph 2d of Enclosure 3 of this instruction.

e. Enter into service-level agreements with the Director, DISA, when necessary, to support validated MP requirements with enterprise-level services. For legacy information sharing networks, implement a migration plan to align these agreements to standards if an exception has been granted.

f. Manage MP information sharing communities for respective Component responsibilities and missions and areas of responsibility (AORs) in accordance with section 1 of Enclosure 3 of this instruction.

g. Use, to the maximum extent possible, capability and associated services for U.S. task forces' support to MPs consistent with Reference (an).

h. Provide candidate enterprise services capabilities, through the DoD CIO Executive Board governance structure, to develop and extend MPE capability.

i. Participate in mission-based interoperability compliance and assessment test and evaluation activities in coordination with DISA, the Combatant Commands, and the CJCS.

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

a. Develops, coordinates, and distributes policies, doctrine, and procedures for the use of MPE information sharing capability in support of joint and combined operations.

b. Co-leads and co-manages the development, evolution, and implementation of MPE electronic information sharing capability through the warfighting mission area portfolio.

c. Co-leads with the DoD CIO the establishment of a centralized MPE governance process.

d. Designates a Principal Accrediting Office (PAO) to ensure guidance across MPEs in support of Phase 0-5 operations.

e. Designates a requirements sponsor in accordance with References (aq) and (ar), to ensure the operational community guides the development of future MPE information sharing capability.

f. Facilitates, through the Joint Requirements Oversight Council and the requirements sponsor designated pursuant to paragraph 9d of this enclosure, the continued validation and integration of evolving MPE information exchange requirements and capabilities in accordance with the Defense Information Enterprise Architecture (DIEA) (Reference (ba)). Supports the guiding principles and priorities of the JIE and capability gaps identified in the FMN initial capabilities document (Reference (bb)) as needed.

g. Participates in MP forums, such as the Combined Communications Electronics Board and Multinational Interoperability Council, and coordinates appropriate actions with DISA and the requirements sponsor as designated in paragraph 9b of this enclosure to promote development of MPE information sharing capability.

h. Assists the DoD CIO in monitoring and evaluating MPE information sharing capability provided by the DoD Components.

i. Directs the evaluation, validation, and prioritization of MPE requirements in accordance with Reference (ad) and Chairman of the Joint Chiefs Instruction 8501.01B (Reference (bc)) for information systems used to share DoD information with MPs. Provides these as input to the DoD CIO and the Director, DISA, to assist in the development, acquisition, deployment, operations, and sustainment of MPE information sharing capability.

j. Coordinates with the DoD CIO, the USD(AT&L), the Commander, U.S. Cyber Command (CDRUSCYBERCOM), the Director, DISA; the Military Departments, and the Commander, United States Special Operations Command (in their Title 10 (service-like role)), to ensure that enterprise services, interface specifications, and standards integrate command and control planning and warfighting applications to support multinational force commander requirements. These requirements are developed following the guidelines and common technical standards provided in References (w) and (ba).

k. Coordinates with the USD(I) to ensure synchronization of intelligence capabilities with operational capabilities for MPE electronic information sharing solutions.

l. Directs the use of a core set of standards for information exchange and applications developed in accordance with Reference (ab) to facilitate unclassified electronic information sharing with MPs.

m. In accordance with Reference (aq), coordinates with the Joint Chiefs of Staff and the MPE requirements sponsor in addressing validated MPE information sharing requirements.

n. Uses MPE electronic information sharing capability during joint exercises and experimentation to promote the development of supporting doctrine; concepts of operation; and tactics, techniques, and procedures (TTP).

o. In coordination with the Combatant Commanders and the Director, DISA, establishes TTPs to encompass MPE information sharing community establishment, maintenance, and termination to include development of service-level agreements and identity management.

p. Establishes a mission-based interoperability compliance and assessment requirements and prioritization process and provides operational direction to the mission-based interoperability compliance and assessment organization. Works with the Combatant Commanders and the Military Departments to establish and manage requirements and priorities.

q. Coordinates MPE requirements that cross Combatant Command, Service, and Defense Agency boundaries. Designates supported (lead) organization and supporting organization for these requirements.

r. In conjunction with the DASD(DT&E), DOT&E, and Director, DISA, supports development of mission-based interoperability methodology for test and evaluation within the MPE environment, focusing on coalition requirements validation and interoperability.

10. COMBATANT COMMANDERS. In coordination with the CJCS and requirements sponsor designated in accordance with paragraph 9d of this enclosure and in addition to the responsibilities in section 8 of this enclosure, the Combatant Commanders:

a. Maintain operational oversight in their respective AORs and integrate the operation and management of MPE electronic information sharing capability in support of regional combined operations as an integrated element of global electronic MPE information sharing capability.

b. Implement and provide accreditation for information systems on networks that support MPE electronic information sharing capability. Exceptions to specifications and standards require DoD CIO approval.

c. Direct the participation of their respective commands in the immediate operational needs and configuration management processes implemented by the solution providers for MPE electronic information sharing capability.

d. Establish and operate an accredited cyberspace defense service provider and operations center for the management, security, and coordination of networks within their AORs unless otherwise provisioned through a solution provider's regional service center.

e. Assist appropriate federal agencies in developing standards for agreements that address electronic information sharing with MPs.

f. Act as the approval authority in their respective AORs in regards to their responsibilities for the establishment, maintenance, and termination of MPE information sharing communities and their membership.

g. Direct commanders to employ the MPE framework for operational information sharing with traditional and non-traditional MP.

h. Manage MPE information sharing communities in their respective AORs by:

(1) Adding or removing partners from existing MP information sharing communities, as necessary. Combatant Commanders will also establish new communities or disestablish existing communities as necessary. They may also help the USD(P) develop any necessary information sharing agreements for their respective MP information sharing communities and coordinating with the other MPE participants.

(2) Developing instructions that provide MPs the required instructions for joining, participating, and exiting MP information sharing communities.

(3) Sponsoring U.S. agencies (other than DoD) to be provided MPE electronic information sharing capability.

(4) Providing DISA access to any authoritative repository of Combatant Command-sponsored users of the MPE electronic information sharing communities and their respective identity and privileges as needed for proper cross-MP information sharing community authentication, access, and privilege management functions.

(5) Establishing and maintaining an existing enterprise infrastructure separate from their headquarters and remote site local area networks, unless otherwise provisioned through a defense enterprise computing center. This multinational enterprise environment will serve as the regional services hub, where appropriate, providing a regional network management connection to DISA and U.S. Cyber Command, as required by DISA for selected networks. This capability will be provided in the DISA-prescribed format for use in global visibility in existing network operations and computer network defense.

i. Provide operational requirements to the Joint Staff for validation and prioritization of mission-based interoperability compliance and assessment efforts supporting Combatant Command objectives.

ENCLOSURE 3

PROCEDURES

1. MP INFORMATION SHARING COMMUNITY MANAGEMENT

a. The MPE framework:

(1) Enables coalition and joint force commanders access to an MPE that supports the required training and the conduct of operations through all five phases (as defined in the Glossary) with any MP at any time.

(2) Provides strategic, operational, and tactical flexibility for all commanders to execute command and control (C2) by providing the means to communicate commander's intent clearly to achieve unified action.

(3) Leverages a federated network concept supporting the connection of multiple networks and national systems with applications and tools to enable MP information sharing within a single security domain for a given operation.

b. An MPE is established within MP agreed-to instructions where individual MPs are resourced and equipped independently, each contributing their own resources to the mission or federated network. The mission environment, whether classified or unclassified, is also capable of securely integrating U.S. and MP C2 and intelligence, surveillance, and reconnaissance infrastructures and authoritative data.

c. The DoD Component heads, who establish an MPE that shares classified military information up to and including SECRET will base the terms of the sharing arrangements on formal agreements with MPs. These formal agreements will ensure information security, information assurance, foreign disclosure (when applicable), and other governance concerns are addressed. The agreements should include instructions for the classification, safeguarding, dissemination, or release of information. These agreements will also include adequate privacy and civil liberties protections and safeguards consistent with References (i) through (k). Reference (ah) will frame the details of information sharing agreements with U.S. partners. References (m), (k), (aa), and (ab) provide guidance for electronic information sharing with U.S. partners. References (y) and (ax) provide guidance for disclosure to foreign partners.

2. STANDARDS AND SPECIFICATIONS

a. The DoD Components will use a core set of standards to facilitate MP electronic information sharing for unclassified operations. Exceptions will:

(1) Be generated by the Joint Staff, the Combatant Commands, the Defense Agencies, or other DoD Components and provide a detailed description and rationale.

(2) Be subjected to a technical review. In accordance with paragraph 2f of Enclosure 2, Director, DISA, will conduct the review and provide a recommendation to the DoD CIO.

(3) Identify a time period in which the exception is valid and a mitigation plan submitted that brings the capability into compliance with standards.

(4) Be directed by the DoD CIO, the Commander, U.S. Strategic Command; or the CDRUSCYBERCOM to shut down the MPE network immediately if mitigation plans are not met.

b. The solution provider will establish MP interface specifications and standards, assessed in accordance with the Risk Management Framework, pursuant to Reference (ah), that:

(1) Permits any organization using established MP interface specifications and standards and possessing the necessary security and access controls and permissions to be globally interoperable with any other similar organization.

(2) Defines the appropriate levels of confidentiality, integrity, availability, authentication, and non-repudiation; provides procedures for using security control implementation MP electronic information sharing operations.

(3) Defines a common, enterprise-level communications and computing architecture to provide the mandated range of information and information management services.

(4) Defines MP information sharing, community-based access controls and identity management services that, when implemented, will enable authorized users to share information appropriately while preventing access by unauthorized users on the same network.

(5) Develops policies for identity authentication and access management that support flexible, responsive electronic information sharing with MP information sharing community members.

(6) Provides guidance and standards to enable development by the DoD Components of interoperable, deployable components for mobile, combined operations with MPs.

(7) Supports regional network architecture to support forward Combatant Command headquarters and split-base operations.

(8) Is widely discoverable through a standards registry, with specific guidance for applications, data, and services for MPE electronic information sharing capability.

(9) Identifies commercial standards to facilitate MP participation and interoperability, to the maximum extent possible.

c. The Combatant Commands and their assigned Service Components will ensure subordinate commands utilize the network standard accreditation. When the Combatant Command or a subordinate command must deviate from the approved baseline, the Combatant Command will submit a request to Director, DISA, for appropriate interoperability testing, certification, and accreditation of the information system. Prior to allowing access by authorized users, the Combatant Commands must accredit the implementation of the networks that support MPE electronic information sharing.

d. Electronic data and information that is intended to be shared should carry tightly bound tags, labels, or metadata containing classification determination, markings, disclosure, and handling rules to support the guidance for information assurance in accordance with Reference (w).

3. GOVERNANCE

a. A centralized MPE governance process established by the DoD CIO and MPE stakeholder community is required to establish policies and issue guidance, provide strategic vision and oversight of the integration and evolution of MPE capabilities, validate requirements, establish and publish joining, membership, and exiting instructions (JMEI), ensure standards compliance, define network architecture, manage configuration control, and validate interoperability of MP networks and systems.

b. When required, the DoD will participate in the MPE governance and management constructs necessitated by non-U.S. led operations.

c. The DoD will designate a PAO for the MPE.

d. The assigned mission commander will appoint a designated approving official for the mission specific network.

e. Security, interconnection, service, data exchange, and metadata standards and specifications will be established and maintained through the appropriate governance forum as described in paragraph a. of this section. To the greatest extent possible, commercial standards will be adopted to improve interoperability.

4. TECHNICAL IMPLEMENTATION OF MPE

a. Infrastructure Support

(1) The JIE, which is composed of shared IT infrastructure, enterprise services, and a single security architecture, will support MP operations, exercises, and training.

(2) The JIE will exist as a separate capability from IT capabilities operated by external MPs. It will provide consistent, standards-based interfaces to improve interoperability and electronic information sharing within the MPE.

(3) Access to data and services will be controlled through the use of DoD designated identity and access management capabilities.

b. Network Federation

(1) Mission networks will be created through the federation of MP networks and systems. The DoD will leverage or re-purpose existing capabilities and will not create or build separate and distinct mission networks to enable the MPE unless authorized by the DoD CIO. Network characteristics are listed in paragraphs 4b(1)(a) and (b):

(a) Phase 0 operations will be supported by an enduring or persistent strategic federated or mission network that facilitates electronic information sharing with specified MPs (bilateral or communities of interest) to support Combatant Command engagements and planning.

(b) Phases 1-5 operations will be supported by an episodic or mission focused operational or tactical federated or mission network that facilitates electronic information sharing with unknown MPs in support of emergent or contingency operations for an unknown period.

(2) MPs will retain full control and responsibility over their portion of the mission network.

(3) MPs will resource and execute all required actions for their portion of the mission network.

(4) Mission networks will be implemented using a single security domain to ensure the uninhibited flow of information and improve interoperability between MPs.

5. JMEI

a. JMEI will guide network federation. At a minimum, the JMEI will encompass the processes and technical aspects required of MPs to connect to, participate in, and disconnect from the mission or federated network.

b. JMEI will be utilized to support operations, exercises, experiments, tests, and training events conducted with MPs.

c. JMEI will be maintained at the UNCLASSIFIED level to facilitate sharing amongst MPs. Portions of the JMEI that require higher classification will be made available through appropriate means.

6. Mission-based Interoperability Compliance and Assessment

a. The mission-based interoperability compliance and assessment capability is required to provide a commander with a high level of confidence that information can be exchanged with whom it is required, when and where it is required, as determined by operational need and the accepted level of risk.

b. Mission-based interoperability assessments will occur before, during, and after mission network implementation to ensure interoperability, functionality, and to exact disciplined change management.

c. Mission-based interoperability assessments will occur in a distributed, operationally relevant, external test and assessment environment. This environment replicates and emulates the desired federated/mission network.

d. Mission-based interoperability compliance and assessment priorities will be determined through a governance and management process.

7. CLASSIFICATION, DISCLOSURE, AND RELEASE

a. The proper classification or designation, disclosure, and release of classified information, including information categorized as unclassified, controlled unclassified, or classified, published on or transmitted through DoD networks is the responsibility of the DoD organization publishing the information and must be accomplished in accordance with Reference (n).

b. Information producers will make provisions for tear line segregation of releasable information when generating data. Handling rules will include a mechanism for filtering releasable information from unreleasable information.

c. The DoD Components will follow the guidelines in References (ab) and (y) for determining disclosure authority and for releasing U.S. classified information when exchanging information with foreign partners, including sharing information on foreign-owned or -controlled information networks.

8. TRANSFER OF UNCLASSIFIED INFORMATION. The proper disclosure or release of controlled unclassified information published on or transmitted through DoD networks is the responsibility of the DoD organization publishing the information. DoD Components will disclose or release this information in accordance with Reference, (i) and other applicable policies and guidance.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

AOR	area of responsibility
C2	Command and Control
CDRUSCYBERCOM	Commander, United States Cyber Command
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CMT	Coalition Mission Threads
CSS	Central Security Service
CTE2	Coalition Test and Evaluation Environment
DASD(DT&E)	Deputy Assistant Secretary of Defense for Developmental Test and Evaluation
DIEA	Defense Information Enterprise Architecture
DI2E	Defense Intelligence Information Environment
DIRNSA/CHCSS	Director National Security Agency/Chief Central Security Service
DISA	Defense Information Systems Agency
DISR	DoD Information Technology Standards Registry
DoD CIO	DoD Chief Information Officer
DoDD	DoD Directive
DoDI	DoD Instruction
DoDIN	DoD Information Network
DOT&E	Director of Operational Test and Evaluation
DSCA	Defense Support of Civil Authorities
E.O.	Executive order
FMN	Future Mission Network
IC	intelligence community
IP	Internet Protocol
ISE-G	Information Sharing Environment Guidance

IT	information technology
JIE	Joint Information Environment
JITC	Joint Interoperability Test Command
JMEI	joining, membership, and exiting instructions
JROCM	Joint Requirements Oversight Council Memorandum
MCO	Major Combat Operations
MP	mission partner
MPE	mission partner environment
MNIS	multinational information sharing
NIEM	National Information Exchange Model
NSA/CSS	National Security Agency/Central Security Service
PAO	Principal Accrediting Office
TTP	Tactics Techniques Procedures
UCDMO	Unified Cross Domain Management Office
U.S.C.	United States Code
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
VPN	virtual private network

PART II. DEFINITIONS

These terms and their definitions are for the purpose of this instruction.

mission-based interoperability compliance and assessment. A mission-based interoperability assessment methodology used to assure and validate operational and technical interoperability, fit for use and purpose, and configuration control on a mission network. Assessments are completed in an external operationally relevant environment. An example of this capability was

instantiated during International Security Assistance Force operations over the Afghanistan Mission Network using the Coalition Interoperability Assurance Validation process.

discovery. The process by which users and applications can find data and services on the Global Information Grid, such as through catalogs, registries, and other search services.

DoDIN. The globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The DoDIN includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems. Non-DoDIN IT includes stand-alone, self-contained, or embedded IT that is not, and will not be, connected to the enterprise network.

enterprise network. A network designated by the DoD CIO Executive Board to provide a defined capability serving the multiple DoD Components. An enterprise network also aligns with DoDIN architecture, as being managed with enterprise-wide oversight, and provides service to any user with a validated requirement.

IT services. The performance of any work related to IT and the operation of IT, including national security systems. This includes outsourced IT-based business processes, outsourced IT, and outsourced information functions.

JIE. A secure joint information environment composed of shared IT infrastructure, enterprise services, and a single security architecture to achieve full spectrum superiority, improve mission effectiveness, increase security, and improve IT efficiency.

JMEI. The processes and technical configurations required of MPs when connecting a MP or national network extension to an event lead's mission network core at a security classification level specific to that event, proposing and implementing changes to services operating within the mission network, and when disconnecting a national extension from a mission network core. The intent of the JMEI is to provide a template for connection of joint services and MPs in a trusted federated mission network that is consistent and coherent across the DoD. JMEI may be utilized as a template to guide establishment of a federation of networks to support any event with a unique security classification level information and data exchange environment shared by all MPs electing to connect.

mission-based interoperability. A mission-focused interoperability methodology that maps the end-to-end flow and exchange of data, assisting in the overall improvement, streamlining, and integration of processes involving operational and technical exchange requirements aligned to specific mission needs. The methodology results in fit for purpose determinations.

multinational. Defined in Joint Publication 1-02 (Reference (bd)).

MNIS Program. The MNIS service facilitates electronic information sharing among DoD Components and eligible foreign nations in support of planning and execution of military

operations. MNIS replaces or consolidates an operational capability equal to or greater than the capability provided by the current operational system.

MP. Those with which the DoD cooperates to achieve national goals, such as other departments and agencies of the U.S. Government; State and local governments; allies, coalition members, host nations and other nations; multinational organizations; non-governmental organizations; and the private sector.

MPE. An operating environment that enables C2 for operational support planning and execution on a network infrastructure at a single security level with a common language. An MPE capability provides the ability for MPs to share their information with all participants within a specific partnership or coalition beginning in Phase 0 and transitioning to execution of Phase 1, Day 1 operations. Formerly FMN.

MP information sharing community. A collaborative group of organizations and users that exchange information within a MPE. MP information sharing community members function as a group because of common standards and protocols and mutual agreements and shared services. MP information sharing communities have previously been referred to as coalitions or communities of interest due to their diverse applications in MP information sharing activities.

network. A set of routing, switching, load balancing, security, and transmission subsystem communications components. Networks can be Internet Protocol (IP)-based, non-IP based, or a combination. Networks can be wired, wireless, terrestrial, airborne, seaborne, satellite, or based on a combination of transport mechanisms and protocols. A network includes all hardware, firmware, and software components residing in routing, switching, load balancing, security, and transmission subsystem communications components themselves, as well as any communications-related hardware, firmware, and software components that reside in supporting hosts (e.g., communications protocols).

network management. The execution of the set of functions required for controlling, planning, allocating, deploying, coordinating, and monitoring the resources of a telecommunications network, including performing functions such as initial network planning frequency allocation, predetermined traffic routing to support load balancing, cryptographic key distribution authorization, configuration management, fault management, security management, performance management, and accounting management. Network Management does not include user terminal equipment.

Phase 0-5. In joint operation planning, a definitive stage of an operation or campaign during which a large portion of the forces and capabilities are involved in similar or mutually-supporting activities for a common purpose. Notional Operation Plan Phases are Phase 0 – Shape, Phase I – Deter, Phase II – Seize Initiative, Phase III – Dominate, Phase IV – Stabilize, Phase V – Enable Civil Authorities.

Risk Management Framework. The unified information security framework for the entire Federal Government that is replacing the legacy Certification and Accreditation processes within Federal Government departments and agencies, the DoD, and the IC. It is is an integral part of

the implementation of the Federal Information Security Management Act, and is based on publications of the National Institute of Standards and Technology and the Committee on National Security Systems.

solution provider. A provider of a new item (including ships, tanks, self-propelled weapons, aircraft, etc., and related spares, repair parts, and support equipment, but excluding real property, installations, and utilities) developed or purchased to satisfy one or more capability requirements (or needs) and reduce or eliminate one or more capability gaps. Solutions may be non-material and might include: changes to doctrine, organization, training, (existing) materiel, leadership and education, personnel, and/or facilities, implemented to satisfy one or more capability requirements (or needs) and reduce or eliminate one or more capability gaps, without the need to develop or purchase a new materiel solution.

tear line. A physical line on an intelligence message or document separating categories of information that have been approved for foreign disclosure and release. Normally, the intelligence below the tear line is that which has been previously cleared for disclosure or release.