DoD Instruction 8110.01

Mission Partner Environment Information Sharing Capability Implementation for the DoD

Originating Component:	Office of the DoD Chief Information Officer
Effective:	June 30, 2021
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Reissues and Cancels:	DoD Instruction 8110.01, "Mission Partner Environment (MPE) Information Sharing Capability Implementation for the DoD," November 25, 2014
Incorporates and Cancels:	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
Approved by:	John B. Sherman, Acting DoD Chief Information Officer

Purpose: In accordance with the authority in DoD Directive (DoDD) 5144.02, this issuance establishes policy and assigns responsibilities for implementation of a mission partner environment (MPE) and MPE capabilities to support unified actions across the full range of military operations.

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

a. This issuance applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands (CCMDs), Office of 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 issuance as the "DoD Components").

b. Nothing in this issuance affects the authorities and responsibilities of the Director of National Intelligence, especially regarding the protection of intelligence sources, methods, and activities from unauthorized disclosure.

1.2. POLICY.

a. To enhance national defense, increase lethality, and strengthen alliances, the DoD promotes effective information sharing, in accordance with applicable Federal laws, policies, and agreements, among mission partners (MPs), which include:

(1) Other Federal departments and agencies.

(2) State, local, and tribal governments and agencies.

(3) Non-government organizations.

(4) Private sector organizations.

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

(6) Multinational treaty.

b. MPE is the operating framework enabling command and control (C2) and information sharing for planning and execution across the full range of military operations. An MPE capability provides the ability for DoD and MPs to exchange information with all participants within a specific partnership or coalition.

c. MPE supports commanders' execution of critical joint warfighting functions: C2, information, intelligence, fires, movement and maneuver, protection, and sustainment. To perform these warfighting functions, commanders require services that are common to both the enterprise and expeditionary levels of operation for human-to-human collaboration (e.g., chat, secure voice, video teleconferencing, email (with or without attachments), web browsing).

d. DoD officials who authorize information sharing will establish, consistent with applicable Federal laws, policies, and agreements, appropriate information-sharing activities that facilitate coordination and cooperation between DoD and MPs to enable a common understanding of the

stabilization and reconstruction, disaster relief, or humanitarian and civic assistance environment and to support an integrated whole-of-government response capability.

e. DoD information is visible, accessible, understandable, linked, trustworthy, interoperable, secure, and made available to appropriate MPs, to the maximum extent allowed by law, National Archives and Records Administration requirements, National Security Policies, National Disclosure Policies, General Security of Military Information Agreements, 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, DoDD 5240.01, DoD Instruction (DoDI) 5400.11, DoDI 5015.02, Office of Management and Budget Memorandum M-19-21, and other Federal laws, Executive orders, and DoD policies regarding the protection of privacy information and civil liberties.

(2) Authorization for secure, efficient, and cost efficient disclosure and handling of classified information, controlled unclassified information, unclassified information, and data shared from and with MPs will be determined in accordance with U.S. law and DoD policies and guidance, including Executive Orders (E.O.s) 12333, as amended, 13526, and 13556; DoDIs 5200.01 and 5200.48; Volumes 1 through 3 of DoD Manual (DoDM) 5200.01; and DoDD 5230.11.

(3) Special emphasis will be placed on protecting information pertaining to U.S. citizens and resident aliens in accordance with DoDI 5400.11, DoD 5400.11-R, DoDM 5240.01, and Section 803 of Public Law 110-53.

f. A common set of standards, protocols, and interfaces will be used to enable the sharing of DoD data, information, and information technology (IT) services in accordance with North Atlantic Treaty Organization (NATO) Federated Mission Networking (FMN) Management Group specifications, DoDI 5400.11, DoD 5400.11-R, DoDM 5240.01, Section 801 of Public Law 110-53, DoDI 8310.01, and DoDI 8551.01.

(1) Pursuant to DoDI 8320.07, the National Information Exchange Model must be considered when deciding which data exchange standards or specifications meet mission and operational needs.

(2) Pursuant to DoDI 8310.01, information-sharing standards will be drawn from approved standards in the Defense Information Technology Standards Registry when applicable, and waiver requests will explain the use of other standards.

(3) 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.

g. The MPE supports DoD digital modernization goals and objectives in concert with initiatives, including Joint All-Domain Command and Control (JADC2), and in alignment with FMN specifications and standards.

h. A coalition interoperability assurance and validation capability, as defined in CJCS Instruction (CJCSI) 5128.02, will be sustained as an enduring capability and will utilize the mission-based interoperability and assessment methodology to support MPE and FMN pursuant to DoDD 5101.22E.

i. The Defense Acquisition System and all DoD Component capability developers will require that U.S. forces maintain coalition interoperability for sharing information and data with MPs through use of appropriate standards and protocols.

j. The institutionalization of MPE within the DoD constitutes using the doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy approach for ensuring the appropriate cultural and joint doctrinal shifts translate to fully trained and equipped U.S. forces ready for the execution of unified actions with MPs across the full range of military operations to meet the commanders' mission objectives.

k. All information and program-generated records, regardless of media or security classification, will be created, maintained and used, disposed, and preserved to document the transaction of business and mission of the program, in accordance with DoDI 5015.02.

l. During stabilization operations, the DoD supports and reinforces the civilian efforts of the U.S. Government lead agencies pursuant to DoDD 3000.05.

m. In response to CCMD-defined and Joint Staff-validated requirements, the DoD may provide military ICT capabilities to share spectrum or bandwidth, and to provide other services that are associated with the ICT infrastructure, including cellular telephone, wireless, and bandwidth, ICT infrastructure services to support stabilization and reconstruction, disaster relief, and humanitarian and civic assistance operations, consistent with applicable legal authority for those operations.

SECTION 2: RESPONSIBILITIES

2.1. DOD CHIEF INFORMATION OFFICER (DOD CIO).

In addition to the responsibilities in Paragraph 2.10., the DoD CIO:

a. Reviews MPE IT development to oversee compliance with enterprise architectures, privacy requirements, and IT standards, including network, cybersecurity, data standards, and related policy requirements. Pursuant to DoDD 8000.01, the DoD CIO, as the Principal Staff Assistant for MPE, and provides oversight for IT compliance.

b. Oversees integration and distribution of MPE and FMN information-sharing standards into the operation of DoD enterprise services in accordance with DoDI 8510.01.

c. Issues DoD guidance, consistent with DoDD 5144.02, 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 DoDIs 8310.01 and 8330.01.

(3) The development and use of data tagging and labeling, multi-level security services, virtual private networks, and confidentiality mechanisms in coordination with the Director, National Security Agency (NSA)/Chief Central Security Service (CSS), the NATO FMN Management Group, and other organizations and standards to promote assured information sharing.

(4) Implementation of the provisions of Information Sharing Environment Guidance 108 and Presidential Memorandum, "Memorandum on Guidelines and Requirements in Support of the Information Sharing Environment," December 16, 2005.

d. In coordination with the DoD Executive Agent (EA) for DoD MPE:

(1) Provides standardized guidance for data exchanged by MPE networks during processing, transport, storage, handling, and distribution.

(2) Requires overall classification markings designated by the original classification authority are maintained in accordance with Volume 2 of DoDM 5200.01.

(3) Develops standardized guidance for use with other Federal departments and agencies regarding data tagging, discovery, and access in accordance with DoDI 8320.07 and consistent with the overall classification marking of the data and the established access privileges of the individual MP.

e. In coordination with DoD EA for DoD MPE and the heads of United States Cyber Command (USCYBERCOM), the Defense Information Systems Agency (DISA), NSA, and

other DoD Components, provides guidance and support for MPE cybersecurity in accordance with DoDIs 8500.01 and 8510.01.

f. When appropriate, assists other Federal departments and agencies to identify and develop strategies for the use of information and communications technology capabilities pursuant to DoDD 3000.05.

g. In coordination with the Director, DISA; Under Secretary of Defense for Intelligence and Security (USD(I&S)); and Under Secretary of Defense for Personnel and Readiness (USD(P&R)) provides DoD policy, technical architecture and designs for DoD enterprise identity, credential, and access management implementation across DoD Components to support MPE.

2.2. DIRECTOR, DISA.

Under the authority, direction, and control of the DoD CIO and in addition to the responsibilities in Paragraph 2.10., the Director, DISA:

a. Provides DoD MPE enterprise-wide network transport and services for voice, data, and video in support of MPE information sharing in accordance with DoDDs 5101.22E and 5105.19.

b. Sustains DISA-managed enterprise information sharing capabilities. In coordination with the DoD EA for DoD MPE, develops, coordinates, and issues technical procedures for the DoD Components to follow when managing and using DISA enterprise information sharing capabilities.

c. Participates in the development of identity, credential, and access management policies that support secured, available, and accurate information sharing with MPs in coordination with the DoD EA for DoD MPE; the DoD CIO; the USD(I&S); the Director, Defense Intelligence Agency; the Under Secretary of Defense for Policy (USD(P)); the CJCS; the USD(P&R); and the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)).

d. In conjunction with the CJCS, the Under Secretary of Defense for Research and Engineering (USD(R&E)), and the Director of Operational Test and Evaluation (DOT&E), supports development of mission-based interoperability methodology for assessing the MPE.

2.3. USD(I&S).

In addition to the responsibilities in Paragraph 2.10., the USD(I&S):

a. Oversees DoD implementation of Intelligence Community Directive 501 and provides additional direction and guidance, as appropriate, for the acquisition, dissemination, and processing of intelligence and intelligence-related information, including the use of FMN standards to enable JADC2 information sharing capabilities.

b. Oversees the exchange of all DoD intelligence and intelligence-related information and sharing agreements to promote sharing across the MPE in accordance with Intelligence Community Directive 501 and DoDD 5143.01.

c. In conjunction with the USD(P), develops, coordinates, and oversees the implementation of DoD policies and security plans and interoperability requirements for sharing intelligence information (including procedures for implementing foreign disclosure and releasability guidance) to promote MPE intelligence-sharing capabilities in accordance with DoDDs 5144.02 and 5230.11, DoDIs 5200.01 and 8330.01, National Disclosure Policy-1, and FMN capabilities.

d. Serves as the DoD senior security official, pursuant to DoDD 5143.01, to develop and integrate risk-managed security and protection policies and programs that provide intelligence information-sharing capabilities across the MPE.

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

f. Provides advice and guidance to the DoD EA for DoD MPE to develop a security classification guide regarding MPE intelligence information-sharing capabilities.

g. Promotes (among defense intelligence and intelligence community elements) the use of approved MPE and FMN interface specifications and standards in systems developed to exchange intelligence information and data pursuant to DoDD 5250.01.

h. Provides outcome-based performance measures in support of national and defense intelligence systems to the DoD CIO and the DoD EA for DoD MPE.

i. Coordinates on all proposed international agreements concerning intelligence and intelligence-related matters in accordance with DoDI 5530.03.

2.4. DIRECTOR, NSA/CHIEF, CSS.

Under the authority, direction, and control of the USD(I&S), pursuant to National Security Directive 42, and in addition to the responsibilities in Paragraph 2.10., the Director, NSA/Chief, CSS:

a. In coordination with the DoD EA for DoD MPE:

(1) 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 capabilities.

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

b. Assists the DoD in the development or selection of efficient and effective cybersecurity solutions that will enable secure electronic information sharing, which includes:

(1) Information discovery.

(2) Dynamic MP information-sharing communities, leveraging the MPE information-sharing community as appropriate.

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

c. Assists in the development of authorization documentation for the solutions recommended for networks that support MPE electronic information sharing.

2.5. USD(P).

In addition to the responsibilities in Paragraph 2.10., the USD(P):

a. Approves all proposed international agreements with policy significance before and after any negotiations are concluded, consistent with DoDIs 2040.02 and 5530.03.

b. Provides direction and guidance, pursuant to National Disclosure Policy-1, DoDD 5230.11, the March 28, 2013 DoD Chief Information Officer Memorandum, and DoDI 2040.02 to oversee effective implementation of DoD policy for disclosing classified military information and controlled unclassified information to foreign partners.

c. Coordinates on DoD classified military information and controlled unclassified information exchange and sharing agreements to be negotiated and concluded with foreign partners consistent with DoDI 5530.03.

d. In coordination with the USD(I&S) to support information sharing with foreign partners and consistent with Volumes 1 through 3 of DoDM 5200.01, DoDIs 2040.02 and 5200.48, and National Disclosure Policy-1, develops DoD plans, policies, and procedures necessary for effective implementation of foreign disclosure policy for classified and controlled unclassified information.

e. Oversees, in coordination with the USD(I&S), the development and distribution of foreign disclosure training requirements throughout the DoD.

f. Pursuant to DoDD 5111.01, supports the MPE by establishing procedures for the DoD to engage with other Federal departments and agencies on execution and protection requirements for campaign and contingency plans.

2.6. USD(P&R).

In addition to the responsibilities in Paragraph 2.10., and in coordination with the DoD EA for DoD MPE; the DoD CIO; the USD(P); the USD(I&S); the Director, DISA; and the CJCS; the

USD(P&R) develops identity, credential, and access management policies that support secured, available, and accurate electronic information sharing.

2.7. USD(A&S).

In addition to the responsibilities in Paragraph 2.10 and in accordance with DoDD 5135.02, the USD(A&S):

a. As the DoD chief acquisition and sustainment officer, supports delivery and sustainment of timely, cost-effective, and uncompromised capabilities, to include MPE, for DoD.

b. In consultation with the DoD EA for DoD MPE, the USD(I&S), and the DoD CIO, leads acquisition and sustainment of timely and cost-effective MPE capabilities.

c. Provides oversight for the acquisition and sustainment of ICT services and capabilities that could be transitioned as enduring (stay-behind) infrastructure to host-nation military or government organizations continuing to support stabilization and reconstruction, disaster relief, and humanitarian-civic assistance activities.

2.8. USD(R&E).

In addition to the responsibilities in Paragraph 2.10 and in accordance with DoDD 5137.02, the USD(R&E):

a. In coordination with the DoD EA for DoD MPE, guides MPE technology development, transition, prototyping, experimentation, and developmental testing activities and programs.

b. In conjunction with the DoD EA for DoD MPE; the CJCS; the DOT&E; and the Director, DISA; supports development of mission-based interoperability methodology for assessing the MPE.

2.9. DOT&E.

The DOT&E:

a. Oversees the conduct of operational test and evaluation (including cybersecurity testing) to assess MPEs consistent with the responsibilities assigned in DoDD 5141.02 and DoD issuances on test and evaluation. For all MPE programs under DOT&E oversight, the threat-representative cybersecurity assessments will be conducted in accordance with the April 3, 2018 DOT&E Memorandum.

b. In conjunction with the DoD EA for DoD MPE; the CJCS; the USD(R&E); and the Director, DISA; supports development of mission-based interoperability methodology for assessing the MPE.

2.10. OSD AND DOD COMPONENT HEADS, EXCEPT FOR DOT&E.

The OSD and DoD Component heads, except for DOT&E:

a. Manage MPE information sharing capabilities in accordance with applicable DoD acquisition and security policies and procedures, DoD digital modernization infrastructure guidelines, and the JADC2.

b. Support the guidance in the CJCS Joint Capabilities Integration and Development System.

c. Coordinate with the DoD EA for DoD MPE and the CJCS in the development of MPE capabilities to promote enhancements across DoD.

d. Require component capability acquisition executives to adopt MPE to achieve coalition interoperability for sharing information and data with MPs by using FMN spiral specifications for capability development.

e. Identify and coordinate sustainment, consolidation, or elimination of existing MPE coalition information-sharing networks through the DoD EA for DoD MPE, including adjustments to legacy funding sources.

f. In coordination with the DoD EA for DoD MPE, plan, program, and budget for component-specific MPE requirements, including functioning as the Commander, Combined Joint Task Force Headquarters or a component of a combined joint task force, while utilizing MPE expeditionary capabilities as a United States mission network contribution.

g. Provide the DoD EA for DoD MPE with information-sharing program information to validate that DoD Component MPE implementation plans adhere to DoD CIO-approved enterprise services, interface specifications, and standards for FMN and MPE information sharing capabilities.

h. Use existing MPE and FMN-compliant enterprise services and interface specifications and standards developed by the DoD EA for DoD MPE for networks that exchange information with MPs. This does not include the U.S. Secret Internet Protocol Router Network, which is outside of the MPE and FMN.

i. Enter into service-level agreements with the DoD EA for DoD MPE, 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.

j. Manage MP information sharing communities for respective component responsibilities and missions and areas of responsibilities (AORs).

k. Provide candidate enterprise services capabilities through the MPE governance structure to develop and extend MPE capability.

l. When appropriate, participate in mission-based interoperability compliance and assessment test and evaluation activities in coordination with the DoD EA for DoD MPE, the CCMDs, and the CJCS, for verification and validation of FMN specifications for coalition information and data-sharing capabilities.

m. Require U.S. forces to be trained and equipped to operate as part of a multinational force to conduct unified actions; to include stability, security, transition, reconstruction, humanitarian assistance, and disaster relief missions; aligned with joint and military service-level MPE doctrine.

n. Comply with the National Information Exchange Model and FMN technical specifications and standards developed by NATO's FMN Management Group.

o. Sponsor CCMD Service Component or MP capability needs submissions.

p. Establish procedures for validating the operational requirements of DoD-provided ICT support to civil-military partners' stabilization and reconstruction, disaster relief, and humanitarian and civic assistance missions. The DoD Component heads will fund such requirements within ceilings specified in budget guidance documents and in accordance with responsibilities contained in DoDD 3025.18, when participating in Defense Support of Civil Authorities missions.

q. Use an MPE electronic information sharing capability during joint and coalition exercises, experimentation, and demonstrations to promote the development of supporting doctrine, such as joining, membership, and exit instructions; mission threads; concepts of operation; and tactics, techniques, and procedures.

r. Provide MPs the necessary guidance to share information effectively through the use of joining, membership, and exit instructions.

s. Pursuant to DoDI 8530.01, identify a DoD Component-level organization responsible for directing, managing, and supporting network operations, cybersecurity activities, and cybersecurity service providers (CSSPs) of MPE networks and systems; must assign CSSPs for MPE networks and systems and exchange information with the designated CSSPs.

t. Submit requests for exceptions to this issuance to the DoD CIO.

2.11. SECRETARY OF THE AIR FORCE.

In addition to the responsibilities in Paragraph 2.10. and as the DoD EA for the DoD MPE, in accordance with DoDD 5101.22E, the Secretary of the Air Force:

a. Executes the role of the DoD EA for the DoD MPE, in accordance with DoDD 5101.22E, to design, implement, operate, resource, and sustain a DoD-wide enterprise-level capability that supports joint and multinational warfighting functional information-sharing requirements with MPs. Determines suitability for continuation, consolidation, or sunset of legacy MPE capability.

b. Establishes and publishes an MPE portfolio management process for MPE enterprise capabilities.

c. In coordination with the OSD and DoD Component heads, assesses MPE expeditionary capabilities aligned and synchronized with the FMN capability to support planning decisions and all elements of the strategic planning, programming, budgeting, and execution process.

d. In coordination with the CJCS and the Secretaries of the Departments of the Navy and Army, evaluates, recommends prioritization, and incorporates requirements, capabilities, and solutions for the integration and evolution of C2 and intelligence information sharing capabilities in a coalition environment. This includes ensuring mission threads, cross-domain solutions and enterprise services, federated mission systems and applications, cybersecurity, and interoperability testing for information-sharing in a coalition environment.

e. Reviews requests submitted by the DoD Component heads and makes recommendations to the DoD CIO regarding exceptions to the use of MPE capabilities for the exchange of DoD information with MPs.

f. As necessary, issues a security classification guide on C2 and intelligence information sharing in a coalition environment (e.g., software, hardware, architectures, configurations) in coordination with the USD(P), the USD(I&S), the CJCS, and the DoD CIO.

g. Distributes the electronic C2 and intelligence coalition information-sharing capability permissions that are authorized in accordance with DoDI 8510.01 and evolving FMN standards.

h. Coordinates with USD(I&S), the DoD Component heads, and sponsors of coalition information-sharing requirements to validate C2 and intelligence information-sharing requirements, in accordance with applicable requirements processes; and facilitates the integrated delivery of C2 and intelligence capabilities.

i. Develops, in coordination with MPE governance structure and accepted by the DoD CIO, metrics and comparison benchmarks for overall MPE implementation and performance (e.g., mission accomplishment, total life-cycle costs, strategic objective achievement, cost/benefit analysis) to determine specific segments or functional areas to target for process improvement.

j. Establishes network connection approval procedures; DoD joining, membership, and exit instructions for MPE enterprise; and user-registration procedures to support the management of MP information-sharing communities' operations in accordance with DoDI 8010.01.

k. Manages cryptographic keying material for DoD EA for the DoD MPE-managed networks and the supporting virtual private network infrastructures for electronic MPE information sharing capabilities.

l. Develops MPE interface specifications and standards aligned and synchronized with FMN spiral specifications as appropriate, and certified in accordance with the DoD Risk Management Framework in accordance with DoDI 8510.01.

m. In coordination with the Commander, USCYBERCOM; the DoD CIO; the Director, NSA/Chief, CSS; and the other DoD Component heads, implements MPE cybersecurity in accordance with DoDIs 8500.01 and 8510.01.

n. Manages a DoD MPE governance process to provide oversight and guidance for resources, network and systems architecture, requirements, cybersecurity, and policy issues, and additional functional areas, as required.

o. Assists the DoD Components in developing the requirements for the military ICT capabilities and associated data and voice services necessary to support stabilization and reconstruction, disaster relief, and humanitarian and civic assistance according to DoDD 3000.05.

p. Utilizes coalition interoperability assurance and validation mission-based interoperability and assessment methodology to support all phases of capability development and sustainment for MPE coalition sharing of information and data.

2.12. CJCS.

In addition to the responsibilities in Paragraph 2.10., the CJCS:

a. Develops, coordinates, and distributes policies, doctrine, and procedures for the use of MPE information-sharing capabilities in support of joint and combined operations, leveraging FMN implementation lessons learned and spiral specifications.

b. Coordinates with the DoD EA for DoD MPE on development of MP and FMN affiliates' capabilities to promote enhancements across DoD.

c. Include the DoD EA for the DoD MPE in C2 and intelligence information-sharing processes.

d. Designates an operational community requirements sponsor in accordance with CJCSI 5123.01H to help guide the development of future, and as appropriate FMN compliant MPE information-sharing capabilities.

e. Participates in MP forums, as appropriate, and coordinates actions with the DoD EA for DoD MPE and the requirements sponsors to promote development of MPE information-sharing capabilities that meet or exceed the FMN spiral specifications.

f. Assists the DoD CIO in monitoring and evaluating MPE information sharing capabilities provided by the DoD Components.

g. Directs the evaluation, validation, and recommended prioritization of MPE requirements in accordance with CJCSIs 6290.01 and 8501.01B for information systems used to share DoD information with MPs. Provides these as input to the DoD CIO, the Director, DISA, and the DoD EA for DoD MPE, to assist in the development, acquisition, deployment, operations, and sustainment of MPE information-sharing capabilities.

h. Coordinates with the DoD CIO; the USD(A&S); the Commander, USCYBERCOM; the DoD EA for DoD MPE; the Director, DISA; the Secretaries of the Military Departments; and the Commander, United States Special Operations Command (with respect to special operations-peculiar administration and support of United States Special Operations Command) to recommend enterprise services and interface specifications, and to integrate C2 and intelligence planning to support multinational force commander requirements.

i. Coordinates with the USD(I&S) to synchronize of intelligence capabilities with operational capabilities for MPE electronic intelligence information-sharing solutions.

j. Supports the use of a core set of standards for information exchange and applications developed in accordance with DoDIs 8310.01 and 8330.01 and FMN specifications to promote information-sharing with MPs.

k. In accordance with CJCSI 5123.01H, coordinates with the MPE requirements sponsor in addressing validated MPE information sharing requirements to meet or exceed FMN spiral specifications.

l. Establishes mission-based interoperability compliance and assessment requirements and prioritization process to include assessments supporting established outcome-based performance measures. Coordinates with the DoD CIO, the USD(I&S), the DoD EA for DoD MPE, the Combatant Commanders (CCDRs) and the Secretaries of the Military Departments to provide operational input to the mission-based interoperability compliance and assessment methodology.

m. In coordination with the DoD EA for DoD MPE, establishes and manages MPE requirements and priorities in accordance with CJSCI 6290.01 and CJCSI 5123.01H.

n. Coordinates MPE requirements that cross DoD Components' boundaries. Designates the supported and supporting organizations for these requirements.

o. In coordination with the DoD EA for DoD MPE, engages in the FMN capability-development process to align MPE capability development with FMN spiral specifications development across the Department.

p. Engages with the DoD EA for DoD MPE, the DoD CIO, the CCDRs, and the Military Service Chiefs in conveying emerging FMN spiral specifications development.

q. Standardizes and enforces common operational mission thread applications to support trans-regional operations, and minimize unique information sharing and data capabilities that negatively impact unified actions.

r. Provides outcome-based performance measures for FMN alignment, joint capability, and functional mission areas.

s. In conjunction with the DoD EA for DoD MPE; the USD(R&E); the DOT&E; and the Director, DISA; supports development of mission-based interoperability methodology for assessing the MPE.

t. Provides guidance and coordination to DoD Components for the generation of coalition-enabled capability requirements and systems performance criteria, to include key performance parameters and key system attributes, during the need generation and capability development process.

2.13. CCDRS.

In addition to the responsibilities in Paragraph 2.10., the CCDRs:

a. Integrate the operation and management of MPE electronic information-sharing capabilities supporting regional combined operations as an integrated element of a global electronic MPE information sharing capability and, as appropriate, in accordance with FMN standards.

b. In accordance with DoDI 8510.01, implement and authorize to operate CCMD-owned information systems on networks that support an MPE electronic information-sharing capability. Requests for exceptions will be coordinated with the MPE Executive Steering Committee to the MPE Senior Leader Board.

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

d. Assist Federal departments and agencies, as appropriate, in developing standards for agreements that address electronic information sharing with MPs.

e. 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.

f. Employ the MPE, and as appropriate FMN, framework at all appropriate echelons of training, exercises, and operations in which MPs are participating.

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

(1) Adding or removing partners from existing MP information sharing communities of interest, as necessary. CCDRs will also establish new communities or disestablish existing communities as necessary. In coordination with the USD(P), develop any necessary information sharing agreements for their respective MP information sharing communities and coordinate with the other MPE participants.

(2) Sponsoring other appropriate Federal departments and agencies for MPE electronic information-sharing capability.

(3) Providing the DoD EA for DoD MPE access to any authoritative repository of CCMD-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.

(4) As appropriate, apply the guidance contained in the October 5, 2020 DoD Senior Information Security Officer memorandum for employing information-sharing capabilities for classified information up to the collateral SECRET level.

h. Provide operational requirements to the Joint Staff for validation and prioritization of mission-based interoperability compliance and assessment efforts supporting CCMD objectives in accordance with CJCSI 6290.01.

2.14. COMMANDER, USCYBERCOM.

In addition to the responsibilities in Paragraphs 2.10. and 2.13., the Commander, USCYBERCOM:

a. Provides the DoD EA for DoD MPE situational awareness and access to regional or theater (Tier II) defensive cyber operations effects incidents, reporting, and mitigations pertaining to releasable networks and mission capabilities across DoD, supporting both localized and trans-regional operations.

b. In conjunction with the DoD EA for DoD MPE, establishes a coordination office for mutual support of global (Tier I) decisions and implementing corrective measures and policies.

c. In coordination with the DoD CIO; the DoD EA for DoD MPE; the Director, DISA; the Director, NSA; and the other DoD Component heads:

(1) Implements MPE cybersecurity in accordance with DoDI 8510.01.

(2) Pursuant to DoDI 8530.01, oversees the implementation and execution of the CSSP approval process and evaluates the effectiveness and performance of CSSPs supporting MPE networks and systems, including the exchange of information with the designated CSSPs.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
AORs	areas of responsibilities
C2	command and control
CCDR	combatant commander
CCMD	combatant command
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff instruction
CSS	Central Security Service
CSSPs	cybersecurity service providers
DISA	Defense Information Systems Agency
DoD CIO	DoD Chief Information Officer
DoD EA	DoD Executive Agent
DoDD	DoD directive
DoDI	DoD instruction
DoDM	DoD manual
DOT&E	Director, Operational Test and Evaluation
E.O.	Executive order
FMN	Federated Mission Networking
ICT	Information and communications technology
IT	information technology
JADC2	Joint All-Domain Command and Control
MP	mission partner
MPE	mission partner environment
NATO	North Atlantic Treaty Organization
NSA	National Security Agency
USCYBERCOM	United States Cyber Command
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USD(R&E)	Under Secretary of Defense for Research and Engineering
USD(P)	Under Secretary of Defense for Policy
USD(P&R)	Under Secretary of Defense for Personnel and Readiness

G.2. DEFINITIONS.

Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

TERM	DEFINITION
coalition interoperability assurance and validation	Defined in CJCSI 5128.02.
Enterprise	Defined in Joint Mission Partner Environment (MPE) Concept of Operations (CONOPS), June 2020.
expeditionary	Defined in Joint Mission Partner Environment (MPE) Concept of Operations (CONOPS), June 2020.
Federation	Association of entities with common goals and objectives, each retaining full control of their own capabilities and affairs.
FMN	A governed conceptual framework consisting of people, processes, and technology to plan, prepare, establish, use, and terminate mission networks in support of federated operations.
FMN affiliates	An organization or nation that performs enduring activities to maintain and further develop the capabilities required to establish and operate mission networks. FMN Affiliates will routinely take part in verification, validation, and collective training events to their forces and assets remain fully interoperable and once they have reached the level of compliance required for the federation of Mission Networks, may become Mission Network Participants.
FMN framework	A governed, managed, and all-inclusive structure providing processes, plans, templates, enterprise architectures, capability components, and tools needed to plan, prepare, develop, deploy, operate, evolve, and terminate mission networks in support of multinational operations in dynamic, federated environments. The FMN framework will provide a permanent ongoing foundation so that mission networks can be established and managed efficiently for the purpose of operations, exercises, training, or interoperability verifications.

TERM	DEFINITION
military ICT	Information systems and communications equipment, primarily commercial-off-the-shelf based, that have been purchased by DoD Components to supplement C2 systems and DoD business process systems; in particular, those that facilitate coordination and cooperation with non-DoD entities and may be used in a stay-behind equipment pool for non-DoD entities. Controlled cryptologic items are not included as potential technologies that may be used in a stay-behind equipment pool for non-DoD entities.
Mission-based interoperability	Defined in CJCSI 5128.02.
MPE	A capability framework that improves partner information-sharing, data exchange and integrated execution through common standards governance and agreed-to procedures. MPE supports commanders' execution of critical joint warfighting functions: C2, information, intelligence, fires, movement and maneuver, protection, and sustainment. To perform these warfighting functions, commanders require services be common to both the enterprise and expeditionary levels of operation for human-to-human collaboration (e.g., chat, secure voice, video teleconferencing, email (with or without attachments), web browsing).
MPE enterprise	Strategic to operational level; U.S.-owned and -operated under U.S. policy and regulations; aligned with U.S. approved standards and protocols; globally integrated; day-to-day operations with most-trusted partners and allies; mostly non-perishable data; risk averse: tighter cybersecurity; data centric.
MPE expeditionary	Operational to tactical level; mission commander governed; operated and aligned with agreed-to standards and protocols; regionally and mission focused; operations with most-trusted partners and allies, including unanticipated MPs; mostly perishable data; risk tolerant: collective management of cybersecurity; data centric.

REFERENCES

Chairman of the Joint Chiefs of Staff Instruction 5123.01H, "Charter of the Joint Requirements Oversight Council (JROC) and Implementation of the Joint Capabilities Integration and Development System (JCIDS)," August 31, 2018

Chairman of the Joint Chiefs of Staff Instruction 5128.02, "Mission Partner Environment Executive Steering Committee; Coalition Interoperability Assurance and Validation Working Group," March 27, 2019

Chairman of the Joint Chiefs of Staff Instruction 6290.01, "Requirements Management Process for Mission Partner Environment," September 17, 2019

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

Director of Operational Test and Evaluation Memorandum, "Procedures for Operational Test and Evaluation of Cybersecurity in Acquisition Programs," April 3, 2018

DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007

DoD Chief Information Officer Memorandum "Adoption of the National Information Exchange Model within the Department of Defense," March 28, 2013

DoD Directive 3000.05, "Stabilization," December 13, 2018

DoD Directive 3025.18, "Defense Support of Civil Authorities (DSCA)," December 29, 2010, as amended

DoD Directive 5101.22E, "DoD Executive Agent (DoD EA) for DoD Mission Partner Environment (MPE)," August 5, 2020

DoD Directive 5105.19, "Defense Information Systems Agency (DISA)," July 25, 2006

DoD Directive 5111.01, "Under Secretary of Defense for Policy (USD(P))," June 23, 2020

DoD Directive 5135.02, "Under Secretary of Defense for Acquisition and Sustainment, (USD(A&S))," July 15, 2020

DoD Directive 5137.02, "Under Secretary of Defense for Research and Engineering (USD(R&E))," July 15, 2020

DoD Directive 5141.02, "Director of Operational Test and Evaluation (DOT&E)," February 2, 2009

DoD Directive 5143.01, "Under Secretary of Defense for Intelligence and Security (USD(I&S))," October 24, 2014, as amended

DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014, as amended

DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992

DoD Directive 5240.01, "DoD Intelligence Activities," August 27, 2007, as amended

DoD Directive 5250.01, "Management of Intelligence Mission Data (IMD) in DoD Acquisition," January 22, 2013, as amended

DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise (DoD IE)," March 17, 2016, as amended

DoD Instruction 2040.02, "International Transfers of Technology, Articles, and Services," March 27, 2014, as amended

DoD Instruction 5015.02, "DoD Records Management Program," February 24, 2015, as amended

DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)," April 21, 2016, as amended

DoD Instruction 5200.48, "Controlled Unclassified Information," March 6, 2020

DoD Instruction 5530.03, "International Agreements," December 4, 2019

DoD Instruction 5400.11, "DoD Privacy and Civil Liberties Programs," January 29, 2019, as amended

DoD Instruction 8310.01, "Information Technology Standards in the DoD," February 2, 2015, as amended

DoD Instruction 8320.07, "Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense," August 3, 2015, as amended

DoD Instruction 8330.01, "Interoperability of Information Technology (IT), Including National Security Systems (NSS)," May 21, 2014, as amended

DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, as amended

DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014, as amended

DoD Instruction 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations," March 7, 2016, as amended

DoD Instruction 8551.01, "Ports, Protocols, and Services Management (PPSM)," May 28, 2014, as amended

DoD Manual 5200.01 Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012, as amended

DoD Manual 5200.01 Volume 2, "DoD Information Security Program: Marking of Information," February 24, 2012, as amended

DoD Manual 5200.01 Volume 3, "DoD Information Security Program: Protection of Classified Information," February 24, 2012, as amended

DoD Manual 5240.01, "Procedures Governing the Conduct of DoD Intelligence Activities," August 8, 2016

DoD Senior Information Security Officer Memorandum, "Threshold Guidance for Implementing Security Mechanisms within Mission Partner Environment Information Domains," October 5, 2020

Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended

Executive Order 13526, "Classified National Security Information," December 29, 2009

Executive Order 13556, "Controlled Unclassified Information," November 4, 2010

Information Sharing Council, Information Sharing Environment Guidance (ISE-G) 108, "Identity and Access Management Framework for the ISE version 1.0," December 19, 2008

Intelligence Community Directive 501, "Discovery and Dissemination or Retrieval of Information within the Intelligence Community," January 21, 2009

Joint Mission Partner Environment (MPE) Concept of Operations (CONOPS), June 2020

National Disclosure Policy-1, "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations," February 14, 2017.

National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information Systems," July 5, 1990

Office of Management and Budget Memorandum M-19-21, "Transition to Electronic Records," June 28, 2019

Presidential Memorandum, "Guidelines and Requirements in Support of the Information Sharing Environment," December 16, 2005

Presidential Memorandum, "Memorandum on Guidelines and Requirements in Support of the Information Sharing Environment," December 16, 2005

Public Law 110-53, Section 803, "Implementing Recommendations of the 9/11 Commission Act of 2007," August 3, 2007

United States Code, Section 552a of Title 5, (also known as "The Privacy Act of 1974")

United States Code, Title 10