DoD Directive 8422.01E

DoD Public Safety Communications Capability

Originating Components:	Office of the DoD Chief Information Officer Office of the Under Secretary of Defense for Acquisition and Sustainment
Effective:	June 8, 2022
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Incorporates and Cancels:	Deputy Secretary of Defense Memorandum, "Management of the Department of Defense Enterprise Mass Warning and Notification Capability," September 11, 2017 DoD Chief Information Officer Memorandum, "Update to Attachment of Deputy Secretary of Defense Memorandum, 'Management of the Department of Defense Enterprise Mass Warning and Notification Capability,' September 11, 2017," February 12, 2018
Approved by:	Kathleen H. Hicks, Deputy Secretary of Defense

Purpose: This issuance:

- Establishes policy and assigns responsibilities for deploying and maintaining DoD public safety (PS) communications (PSC) capability and information technology (IT) to support PS, law enforcement and physical security, fire and emergency services, emergency management (EM), and related missions (referred to collectively in this issuance as "PS missions") in accordance with Sections 113 and 191 of Title 10, United States Code (U.S.C.); Section 11315 of Title 40, U.S.C.; and Sections 3102, 3506, and 3544 of Title 44, U.S.C.
- Defines the:
  - Management structure for IT supporting PS missions.
  - Requirements and responsibilities relevant to IT supporting PS missions contained in DoD Instructions (DoDIs) 6055.06, 6055.17, and 8110.01.
- Designates the Secretary of the Army (SECAR) as the DoD Executive Agent (EA) for the emergency mass warning notification (EMWN) system in accordance with DoD Directive (DoDD) 5101.01.

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

a. This issuance applies to:

(1) OSD, the Military Departments (including the Coast Guard at all times, including when it is a Service in the Department of Homeland Security by agreement with that Department), the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the 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").

(2) All military installations worldwide. Implementation of these provisions at military installations outside the United States requires arrangements or formal agreements with host-nation authorities and allied and coalition forces in accordance with DoDI 5530.03.

(3) All DoD IT supporting PS and related operations, including:

(a) Installation security.

(b) Defense support of civil authorities.

(c) Humanitarian assistance.

(d) Disaster recovery.

(e) Incident management.

(f) Mutual aid.

b. This issuance supplements but does not repeal the responsibilities or requirements established for the fire and emergency services or EM programs defined in:

(1) Presidential Policy Directive-8.

(2) DoDIs 5200.01, 5200.48, 6055.06, and 6055.17.

1.2. POLICY.

DoD PSC capability will:

a. Be based on a joint enterprise approach to IT supporting global PS missions to enable efficient and effective operations.

b. Be in accordance with:

(1) Presidential Policy Directive-8.

(2) DoDIs 3020.45, 5200.01, 5200.08, 5200.48, 6055.06, 6055.17, 8110.01, 8500.01, and 8530.01.

c. Support all DoD personnel and related individuals, including:

(1) Active and Reserve Component military personnel and DoD civilian employees.

(2) DoD and non-DoD tenants.

(3) In-transit DoD and U.S. Government personnel.

(4) Dependents of DoD personnel, DoD contractors, visitors, and guests living or working on military installations worldwide.

d. Ensure that IT used for DoD PSC:

(1) Has capabilities equivalent to and compatible with those provided by Federal, State, local, tribal, and host-nation first responders.

(2) Is survivable, resilient, and enduring against all hazards to the extent needed to support PS.

(3) Is in accordance with DoDD 3025.18 and DoDI 8110.01 to enable DoD assistance to civil authorities under:

(a) Mutual-aid agreements.

(b) Host-nation support agreements.

(c) Defense support of civil authorities operations.

(d) Humanitarian assistance and disaster relief.

(4) Operates with Federal, State, local, tribal, territorial, and host-nation first responders, as applicable, including State and local emergency service Internet Protocol (IP) networks, in accordance with DoDIs 4650.10 and 8330.01.

(5) Shares essential information, as appropriate, with Federal, State, local, tribal, territorial, and host-nation mission partners in accordance with DoDIs 5200.01, 5200.48, and 8110.01.

(6) Protects personally identifiable information and protected health information, pursuant to Section 552a of Title 5, U.S.C. and Public Law 104-191, in DoD and mission-partner IT systems in accordance with DoDIs 5400.11, 6025.18, 8530.01, and 8582.01.

(7) Integrates new and emerging PSC technologies within and throughout the DoD and associated communities, when appropriate.

(8) Enables seamless PSC based on the National Emergency Number Association i3 Standard for Next Generation 9-1-1.

(9) Aligns with the National Incident Management System.

(10) Enables the rapid adoption of proven solutions through DoD Component risk-management framework processes and products in accordance with DoDI 8510.01.

e. Transfer benefits from the DoD's research, development, and test and evaluation capabilities, including technology transfers, to mission partners, to the greatest extent practical, in accordance with DoDI 5535.08.

f. Be delivered by IT operated by DoD Components, civilian mission partners, or a combination thereof.

SECTION 2: RESPONSIBILITIES

2.1. DOD CIO.

The DoD CIO:

a. Oversees DoD PSC IT activities and performs DoD PSC IT investment oversight functions.

b. Co-chairs the DoD PSC Senior Steering Group (PSCSSG).

c. Establishes the reference architecture for PSC.

d. Serves as the Principal Staff Assistant (PSA) overseeing the activities of the DoD EA of the EMWN system and the DoD PSC IT ecosystem in accordance with DoDD 5144.02.

2.2. DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA).

Under the authority, direction, and control of the DoD CIO, and in addition to the responsibilities in Paragraph 2.7., the Director, DISA:

a. Assigns a representative to the PSCSSG.

b. Designates an office of primary responsibility for DoD PSC IT, with a manager at the O6 or GS-15 level or higher, to oversee implementation of and compliance with this issuance.

c. Provides technical oversight and enterprise implementation updates to the PSCSSG as required.

d. Coordinates with the Combatant Commanders to implement this issuance.

e. Has the roles, responsibilities, and authorities for implementing the DoD PSC IT ecosystem specified in Section 3.

2.3. UNDER SECRETARY OF DEFENSE FOR ACQUISITION AND SUSTAINMENT (USD(A&S)).

The USD(A&S):

a. Co-chairs the PSCSSG.

b. In accordance with DoDI 8130.01, develops and maintains standards for PS location, street, and building addressing map data for all DoD facilities. This ensures that PS answering points (PSAPs), emergency call centers (ECCs), and mission partners have access to valid addresses to enable accurate emergency dispatching of first responders.

c. In accordance with DoDI 6055.17, validates functional requirements for IT supporting PS.

2.4. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY.

The Under Secretary of Defense for Intelligence and Security:

a. Assigns a representative to the PSCSSG.

b. Assesses DoD PS information for inclusion into existing Federal and DoD-controlled unclassified information categories or creating a new category.

c. Provides oversight of PSC compliance with DoDIs 5200.01, 5200.08, and 5200.48.

d. In coordination with the DoD CIO, advises on DoD PSC IT enterprise standards to ensure consistency with information security requirements in accordance with DoDI 5200.01.

e. Coordinates with the DoD Components to implement requirements for PS information in accordance with DoDIs 5200.01 and 5200.48, as required.

f. Validates functional security requirements for IT supporting PS in accordance with DoDI 6055.17.

2.5. UNDER SECRETARY OF DEFENSE (COMPTROLLER)/CHIEF FINANCIAL OFFICER, DEPARTMENT OF DEFENSE (USD(C)/CFO).

The USD(C)/CFO:

a. Assigns a representative to the PSCSSG.

b. Supports the DoD CIO in ensuring that the DoD Components plan, program, budget, and allocate resources necessary for the implementation of DoD PSC IT.

2.6. UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS.

The Under Secretary of Defense for Personnel and Readiness:

a. Assigns a representative to the PSCSSG.

b. Coordinates with the:

(1) Assistant Secretary of Defense for Sustainment on EM program matters of mutual interest as they relate to PS programs and activities.

(2) DoD CIO and DISA on the response readiness of IT systems supporting PSC activities.

2.7. DIRECTORS OF THE DEFENSE AGENCIES AND DOD FIELD ACTIVITIES WITH RESPONSIBILITIES FOR PS, PSAPS, OR ECCS.

The Directors of the Defense Agencies and DoD Field Activities with responsibilities for PS, PSAPs, or ECCs:

a. Assign a representative from their respective Defense Agency or DoD Field Activity to the PSCSSG.

b. Develop guidance and procedures, as appropriate, to implement this issuance throughout all installations under their responsibility.

c. Provide sufficient financial and personnel resources to implement and sustain the capabilities described in this issuance across their organizations.

d. Coordinate with DISA for DoD PSC IT.

2.8. SECRETARIES OF THE MILITARY DEPARTMENTS AND THE COMMANDANT OF THE U.S. COAST GUARD.

The Secretaries of the Military Departments and the Commandant, U.S. Coast Guard:

a. Assign a representative from their respective Military Service to the PSCSSG.

b. Designate an office of primary responsibility for PSC, with a manager at the O6 or GS-15 level or higher, to oversee implementation of and compliance with this issuance.

c. Implement guidance and procedures, as appropriate, to ensure compliance with this issuance throughout all installations under their responsibility.

d. Plan for future requirements related to wired and wireless next-generation 9-1-1 (NG911) solutions supporting PS that impact military installations. Provide sufficient financial and personnel resources to implement and sustain the capabilities described in this issuance across their Military Services and supported Combatant Commands.

e. Coordinate with DISA for DoD PSC IT.

2.9. SECAR.

Section 4 specifies the SECAR's roles, responsibilities, and authorities as the DoD EA of EMWN. The SECAR also has the responsibilities that Paragraph 2.8. assigns.

2.10. CHIEF, NATIONAL GUARD BUREAU.

The Chief, National Guard Bureau:

a. Assigns a representative to the PSCSSG.

b. Uses existing infrastructure and personnel to survey DoD PSC IT implementation and compliance with this issuance.

c. Coordinates with State adjutant generals, as appropriate, to voluntarily incorporate this issuance into the State's PS efforts on their installations.

d. Communicates with State and local authorities regarding how DoD PSC IT services would be used during emergencies.

2.11. CHAIRMAN OF THE JOINT CHIEFS OF STAFF.

The Chairman of the Joint Chiefs of Staff:

a. Assigns a co-chair to the PSCSSG.

b. Coordinates with the Combatant Commanders to implement this issuance.

2.12. COMBATANT COMMANDERS.

The Combatant Commanders implement this issuance within their respective areas of responsibility, as appropriate.

SECTION 3: DOD PSC IT ECOSYSTEM

The Director, DISA:

a. Has the roles, responsibilities, and authorities for the implementation of enterprise DoD PSC IT architecture (referred to collectively with DoD Component material capabilities in this issuance as the "DoD PSC IT ecosystem").

b. Is the milestone decision authority for the DoD PSC IT ecosystem.

c. Oversees, coordinates, and develops a process to adjudicate all DoD PSC IT ecosystem issues. Establishes or uses existing working groups comprising representatives from appropriate DoD Components. Charters a change management board for the DoD PSC IT ecosystem. Leverages the range of technologies and mobile communications applications in accordance with changes to policy. Provides monthly written updates to the DoD CIO and updates to the PSCSSG.

d. Provides DoD PSC IT ecosystem funding strategies in coordination with the PSCSSG and the command, control, and communications (C3) leadership board. This includes recommending funding strategies necessary to sustain the DoD PSC IT ecosystem management functions to meet stakeholder requirements.

e. Develops and executes strategic human capital management plans to ensure that the DoD PSC IT ecosystem office is properly staffed with employees with the necessary skills and competencies needed to perform the mission requirements.

f. Leverages the PSCSSG and C3 leadership board governance processes for the integration and evolution of the DoD PSC IT ecosystem in coordination with all PS stakeholders.

g. Appoints an authorizing official for networks that support the DoD PSC IT ecosystem in accordance with DoDIs 5015.02, 8010.01, 8100.04, 8500.01, and 8510.01.

h. Monitors and evaluates the DoD PSC IT ecosystem mission effectiveness provided to the DoD Components.

i. Establishes and maintains records management procedures for protecting, maintaining, and archiving DoD records within the DoD PSC IT ecosystem portfolio in accordance with DoDI 5015.02.

j. Coordinates with the USD(A&S) on programs, policies, and activities pertaining to the DoD PSC IT ecosystem involving acquisition, attaining goods and services, research and development, developmental testing, and contracting strategy.

k. Supports the DoD CIO in ensuring that the DoD Components plan, program, budget, and allocate resources necessary for the implementation of the DoD PSC IT ecosystem.

l. Provides a reimbursable service offering for enterprise-level development, integration, systems engineering, and delivery of mission and enterprise services in support of interagency,

strategic, allied, multinational, coalition, joint, and combined coalition information sharing capabilities in accordance with DoDI 8320.07 and the Unified Capabilities Requirements 2013, including cybersecurity and interoperability testing.

m. Provides reimbursable service offering for DoD enterprise–level C3 capabilities, cross-domain solutions, and transport services used for voice, data, and video in support of the DoD PSC IT ecosystem, in accordance with DoDD 5105.19. The Director, DISA remains the authorizing official for all DISA capabilities and services and provides all network engineering support, computing services, cybersecurity, and localized technical assistance in support of Combatant Commanders.

n. Develops an interoperability test plan with Federal and State interoperability test labs and the Joint Interoperability Test Command. The Joint Interoperability Test Command conducts coalition, multinational, and bilateral operational test and evaluation for PSC capabilities in accordance with DoDI 8100.04.

o. Develops a plan to upgrade all DoD facilities to NG911 through PSAP technology upgrades. This includes transition plans for time-division multiplexing to IP systems and an interim plan to maintain 9-1-1 services during this migration.

p. Develops a DoD PSC IT ecosystem strategy and plan, including evaluating cloud computing solutions through the adaptive acquisition framework in accordance with DoDI 5000.02.

q. Develops a plan for implementing an emergency services IP network (ESInet). Includes the network design and establishing requirements and policies in this plan. Includes in the design a DoD information network mission-partner gateway, a technology refresh requirement for State ESInet peering, and a Zero Trust Network for protecting 9-1-1 call data and location information for interconnections with all DoD PSAPs.

r. Develops a strategy to transition legacy fire and burglar alarm sensors and panels and cameras systems from time-division multiplexing systems to a secure and modernized PSC IT system.

s. Develops a strategy for incorporating emerging PS long-term evolution solutions, land mobile radio, high-frequency radio systems, and mobile satellite systems into the DoD PSC ecosystem.

t. Coordinates with and supports the DoD EA of the EMWN system in integrating this program into the DoD PSC IT ecosystem.

SECTION 4: DOD EMWN

The SECAR:

a. Is the DoD EA of the EMWN system in accordance with DoDD 5101.01.

b. Manages the DoD EMWN system through a program office with these requirements, roles, and responsibilities:

(1) Ensures multi-DoD Component participation.

(2) Is headed by a DoD civilian program executive officer.

(3) Conducts EMWN system planning, resource programing, budgeting, acquisition, deployment, and maintenance.

(4) Integrates across the EMWN system infrastructure.

(5) Oversees EMWN system modernization in coordination with the PSA, DoD Components, and DISA.

c. Plans and implements the directed EMWN system initial and immediate actions and deliverables:

(1) Assesses the costs and resources required to carry out the assigned responsibilities, functions, and authorities.

(2) Develops a prioritized EMWN system resource plan so that the USD(C)/CFO may reprogram or realign funds as necessary.

(3) Coordinates with the Director, Cost Assessment and Program Evaluation for initial minimum funding estimates for the DoD EA to establish the program office and begin planning functions.

(4) Develops a project plan for PSA approval.

(5) Reviews DoD Component budgets and spending plans and makes recommendations as part of the program and budget review process.

d. Develops an overarching EMWN system management and governance structure:

(1) Is the milestone decision authority for the DoD EMWN system.

(2) Oversees, coordinates, and develops a process to adjudicate all designated EMWN system issues.

(3) Establishes working groups or uses existing working groups consisting of appropriate DoD Components representatives.

(4) Charters a change management board for EMWN system capabilities and leverages the range of technologies and mobile communications applications in accordance with changes to policy.

(5) Provides monthly written updates to the PSA and updates to the PSCSSG and the mission assurance coordination board.

e. Coordinates and integrates acquisition and programmatic activities for a DoD-wide EMWN system capability conforming to:

(1) Policies and procedures of the broader DoD EM program in accordance with DoDI 6055.17.

(2) The DoD EA authority to directly request information on existing DoD Component EMWN system capabilities.

f. Develops a plan to implement the initial deployment priority of locations not on main installations (e.g., recruiters, Reserve Component members).

g. Develops a plan to implement the EMWN system with program capability priorities:

(1) Speed of alert.

(2) Cost effectiveness.

(3) Rapid fielding.

(4) Commercially available technology, as practical.

(5) Leveraging rapid acquisition authorities.

(6) Minimizing unnecessary acquisition changes in program scope.

(7) Implementing the plan with existing resources.

h. Develops a fully operational capabilities requirement to provide service to:

(1) Approximately four million personnel, including active duty and Reserve Component Service members, DoD civilians, dependents, and contractors.

(2) Approximately 12,000 locations, including camps, posts, stations, bases, armories, leased facilities, and recruiting stations.

i. Develops an EMWN system that meets alert notification requirements specified in DoDI 6055.17.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
C3	command, control, and communications
CIO	chief information officer
DISA	Defense Information Systems Agency
DoDD	DoD directive
DoDI	DoD instruction
EA	executive agent
ECC	emergency call center
EM	emergency management
EMWN	emergency mass warning notification
ESInet	emergency services Internet Protocol network
GS	General Schedule
IP	Internet Protocol
IT	information technology
NG911	next-generation 9-1-1
PS	public safety
PSA	Principal Staff Assistant
PSAP	public safety answering point
PSC	public safety communications
PSCSSG	public safety communications senior steering group
SECAR	Secretary of the Army
U.S.C.	United States Code
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(C)/CFO	Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense

G.2. DEFINITIONS.

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

TERM	DEFINITION
9-1-1 solutions	Any technology, equipment, personnel, or process that supports an end user's ability to make a 9-1-1 call and connect to a PSAP.
ECC	A building or portion of a building specifically configured for the primary purpose of providing emergency communications or PSAP services to one or more PS agencies under the authority or authorities having jurisdiction.
EM	Defined in DoDI 6055.17.
ESInet	A privately managed IP transport network that many agencies may share.
first responders	Personnel performing mitigation, response, and recovery tasks at one or more incident scenes, including any area directly related to the incident site and, therefore, under the authority over the incident or unified commander.
IT	Defined in Committee on National Security Systems Instruction No. 4009.
military installation	A military installation is a base, camp, post, station, yard, center, homeport facility for any ship, or other area under the jurisdiction of the Secretary of a Military Department or the Secretary of Defense, including any leased location, or in the case of an activity in a foreign country, any area under the operational control of the Secretary of a Military Department or the Secretary of Defense, without regard to the duration of operational control.
NG911	The set of network elements, software applications, databases, customer equipment components, and operations and management procedures required to provide next-generation emergency services.
PS	Activities to keep a covered population protected from dangers affecting safety such as crimes, accidents, or disasters that are typically conducted by first-responder organizations such as police, fire, and emergency medical services.
PSAP	A facility equipped and staffed to receive 9-1-1 calls.

TERM	DEFINITION
PSC	Any voice, text, video, or imagery communicated via an information system or network that supports law enforcement, fire and rescue services, emergency medical response, and EM operations on a military installation. Communications may be between individuals or system to system and may be contained within the installation or to mission partners outside the DoD to support mutual-aid agreements, defense support to civil authorities, and other joint-response operations.

REFERENCES

Committee on National Security Systems Instruction No. 4009, "Committee on National Security Systems (CNSS) Glossary," current edition

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

DoD Directive 5101.01, "DoD Executive Agent," February 7, 2022

DoD Directive 5105.19, "Defense Information Systems Agency," February 15, 2022

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

DoD Instruction 3020.45, "Mission Assurance Construct," August 14, 2018, as amended

DoD Instruction 4650.10, "Land Mobile Radio (LMR) Interoperability and Standardization," July 28, 2015, as amended

DoD Instruction 5000.02, "Operation of the Adaptive Acquisition Framework," January 23, 2020, 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 5200.08, "Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB)," December 10, 2005, as amended

DoD Instruction 5200.48, "Controlled Unclassified Information (CUI)," March 6, 2020

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

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

DoD Instruction 5535.08, "DoD Technology Transfer (T2) Program," May 14, 1999, as amended

DoD Instruction 6025.18, "Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule Compliance in DoD Health Care Programs," March 13, 2019

DoD Instruction 6055.06, "DoD Fire and Emergency Services (F&ES) Program," October 3, 2019

DoD Instruction 6055.17, "DoD Emergency Management (EM) Program," February 13, 2017, as amended

DoD Instruction 8010.01, "Department of Defense Information Network (DODIN) Transport," September 10, 2018

DoD Instruction 8100.04, "DoD Unified Capabilities (CA)," December 9, 2010

DoD Instruction 8110.01, "Mission Partner Environment Information Sharing Capability Implementation for the DoD," June 30, 2021

DoD Instruction 8130.01, "Installation Geospatial Information and Services (IGI&S)," April 9, 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)," April 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 8582.01, "Security of Non-DoD Information Systems Processing Unclassified Nonpublic DoD Information," December 9, 2019

National Emergency Number Association, "National Emergency Number Association i3 Standard for Next Generation 9-1-1," June 14, 2011, as amended

Office of the DoD Chief Information Officer, "Unified Capabilities Requirements 2013 (UCR 2013)," current edition

Presidential Policy Directive-8, "National Preparedness," March 30, 2011

Public Law 104-191, "Health Insurance Portability and Accountability Act of 1996," August 21, 1996

United States Code, Title 5, Section 552a

United States Code, Title 10

United States Code, Title 40, Section 11315

United States Code, Title 44