



DoD INSTRUCTION 4650.08

POSITIONING, NAVIGATION, AND TIMING (PNT) AND NAVIGATION WARFARE (NAVWAR)

Originating Component: Office of the Chief Information Officer of the Department of Defense

Effective: December 27, 2018

Releasability: Cleared for public release. Available on the Directives Division Website at <http://www.esd.whs.mil/DD/>.

Reissues and Cancels: DoD Instruction 4650.08, "Positioning, Navigation, and Timing (PNT) and Navigation Warfare (Navwar)," February 5, 2015

Approved by: Essye B. Miller, Acting Chief Information Officer of the Department of Defense

Purpose: In accordance with the authority in DoD Directive (DoDD) 5144.02, this issuance implements PNT policy pursuant to DoDD 4650.05 and establishes policy, assigns responsibilities, and provides procedures for:

- Integrating PNT and NAVWAR across the DoD pursuant to DoDD 4650.05 and DoD Instruction (DoDI) 5000.02.
- Ensuring the security of PNT information related to the development, acquisition, sustainment, and operational use of PNT information sources and PNT information-dependent systems pursuant to DoDD 4650.05, DoDI 5000.02, and DoDI 8500.01.
- Determining NAVWAR policy compliance and assessing NAVWAR capabilities for programs producing or using PNT information.

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION	3
1.1. Applicability.	3
1.2. Policy.	3
SECTION 2: RESPONSIBILITIES	4
2.1. DoD Chief Information Officer (DoD CIO).....	4
2.2. USD(A&S).....	4
2.3. Under Secretary of Defense for Research and Engineering (USD(R&E)).....	5
2.4. USD(P).....	5
2.5. DOT&E.....	5
2.6. Director, National Reconnaissance Office (NRO).....	5
2.7. Director, Defense Intelligence Agency (DIA).....	6
2.8. DIRNSA/CHCSS.....	6
2.9. Director, Defense Security Cooperation Agency.....	7
2.10. Secretaries of the Military Departments	7
2.11. CJCS.	8
2.12. CDRUSSTRATCOM.	8
2.13. Commander, United States Cyber Command (CDRUSCYBERCOM).	9
SECTION 3: NAVWAR COMPLIANCE PROCEDURES	10
3.1. Discussion.....	10
3.2. Capability Development and System Integration.	10
3.3. Developmental and Operational Test and Evaluation.	11
3.4. Modification of Fielded PNT Capabilities and Aquisitions Outside the Defense Acquisition System.	11
a. Combat, Combat Support, and Combat Service Support.....	12
b. Non-Combat Operations.....	12
GLOSSARY	13
G.1. Acronyms.....	13
G.2. Definitions.....	14
REFERENCES	15

TABLES

Table 1. Notional PNT Conditions and Capabilities for NAVWAR Compliance	11
---	----

FIGURES

Figure 1. NAVWAR Compliance Process Components	10
--	----

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY. This issuance applies to OSD, the Military Departments (including the Coast Guard at all times, including when it is a Service in the Department of Homeland Security), 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 issuance as the “DoD Components”).

1.2. POLICY.

a. The DoD will effectively employ NAVWAR capabilities to ensure a PNT advantage in support of military operations. DoD will use NAVWAR to ensure DoD use of and prevent adversary use of PNT information through coordinated employment of space, cyberspace, and electronic warfare operations.

b. Programs producing or using PNT information must be NAVWAR-compliant in accordance with this issuance, and will report NAVWAR compliance to the Milestone Decision Authority (MDA) at each acquisition program milestone in accordance with DoDD 5144.02 and DoDI 5000.02.

c. NAVWAR compliance effectiveness, including vulnerabilities associated with reliance on a single source of PNT information, will be assessed during plan development for tests, training, exercises, and operations employing PNT information. Section 3 of this issuance describes a compliance process for NAVWAR defensive capabilities (e.g., anti-jam antennas, complementary PNT sources), which must operate in the presence of offensive NAVWAR operations (e.g., jamming, cyber threats). All systems that use PNT information, whether or not the system is under Director of Operational Test and Evaluation (DOT&E) oversight, should be tested in a realistic NAVWAR environment.

d. Reliance on civil, commercial, or foreign sources as the primary means of obtaining PNT information for combat, combat support, or combat service support operations is **not** authorized without a waiver in accordance with CJCS Instruction (CJCSI) 6130.01F. These systems may be utilized as complementary sources, subject to successful NAVWAR compliance determination.

e. Use of civil, commercial, or foreign sources to obtain PNT information for non-combat operations is authorized, subject to successful NAVWAR compliance determination.

f. Through existing information and technology transfer control processes, DoD will ensure a PNT information advantage for U.S. and allied forces.

g. Access to DoD PNT services by U.S. Federal civil agencies and foreign government entities may be authorized in accordance with Paragraph 2.1.e. Access must be approved consistent with applicable U.S. laws, regulations, and DoD policy, including DoD policies for disclosure of classified military information to foreign entities in DoDI 5230.11, and international transfers of technology, articles, and services in DoDI 2040.02.

SECTION 2: RESPONSIBILITIES

2.1. DOD CHIEF INFORMATION OFFICER (DOD CIO). The DoD CIO:

- a. Establishes and implements DoD strategy and policy related to PNT as part of the DoD Information Enterprise in accordance with DoDD 5144.02 and DoDD 3100.10.
- b. In accordance with DoDI 5000.02 and DoDI 4650.06, develops and oversees implementation and coordination of PNT and NAVWAR policy through coordinated actions assigned by the DoD PNT Executive Management Board and Oversight Council.
- c. Oversees the development and publication of DoD PNT and NAVWAR strategy in support of National Security and military strategy.
- d. Assigns responsibilities for determining NAVWAR policy compliance and assessing NAVWAR capabilities for programs producing or using PNT information.
- e. Establishes guidance for PNT and NAVWAR support to U.S. federal agencies and for international cooperation, including policy governing assignment of cryptographic (crypto) networks that support allied and coalition operations, exercises, training, and research and development (R&D) efforts. The DoD CIO coordinates the development of such guidance with the:
 - (1) Under Secretary of Defense for Policy (USD(P)).
 - (2) Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)).
 - (3) Under Secretary of Defense for Intelligence (USD(I)).
 - (4) CJCS.
 - (5) Secretaries of the Military Departments.
 - (6) Commander, United States Strategic Command (CDRUSSTRATCOM).
 - (7) Commander, United States Cyber Command (CDRUSCYBERCOM).
 - (8) Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS).

2.2. USD(A&S). The USD(A&S):

- a. Incorporates DoD CIO guidance for PNT and NAVWAR into acquisition and sustainment programs for systems that produce or use PNT information.
- b. For programs for which the USD(A&S) is the MDA, oversees acquisition and sustainment-related PNT and system-level architecture issues.

- c. Ensures acquisition and sustainment programs are NAVWAR-compliant in accordance with this instruction.
- d. Ensures all DoD systems producing or using PNT information are tested in a NAVWAR environment in coordination with the DOT&E and the DoD CIO.
- e. In coordination with the DoD CIO, updates DoDI 5000.02, and other supporting guidance as appropriate, to incorporate requirements for MDA determination of NAVWAR compliance at system acquisition milestones.
- f. When acting as MDA, determines and confirms NAVWAR compliance at each acquisition milestone for all platforms and systems producing or using PNT information.

2.3. UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING (USD(R&E)). The USD(R&E):

- a. Incorporates DoD CIO guidance for PNT and NAVWAR into R&D programs for systems that produce or use PNT information.
- b. Reviews test and evaluation plans of acquisition programs for which the USD(A&S) is the MDA to ensure they are sufficient to validate platform or system NAVWAR compliance standards.

2.4. USD(P). The USD(P):

- a. Provides oversight and guidance to the DoD CIO on international matters as they pertain to this issuance, including oversight and guidance relating to exports and technology transfers of PNT systems and associated technologies.
- b. Coordinates with the DoD CIO on items identified in Paragraph 2.1.e.

2.5. DOT&E. The DOT&E:

- a. Coordinates with the USD(A&S) and the DoD CIO to ensure all DoD systems under DOT&E oversight that use PNT information are tested in an operationally realistic NAVWAR environment.
- b. For all DoD systems under DOT&E oversight, reviews and approves operational test and evaluation plans to ensure they are adequate to assess PNT and NAVWAR effectiveness, suitability, and survivability.

2.6. DIRECTOR, NATIONAL RECONNAISSANCE OFFICE (NRO). Under the authority, direction, and control of the USD(I), the Director, NRO:

a. Documents NAVWAR electronic warfare support (ES) requirements pursuant to Intelligence Community Directive 115 and CJCSI 3170.01I. Coordinates ES requirements with the CJCS, the Combatant Commanders (CCDRs), the Secretaries of the Military Departments, and the DIRNSA/CHCSS.

b. Provides technical assistance and subject matter expertise to support the Secretaries of the Military Departments as they develop and deploy NAVWAR ES-related capabilities and associated doctrine.

c. For NRO programs fully funded outside of the DoD, considers and documents completion of NRO system-equivalent activities in accordance with Section 3 of this issuance..

2.7. DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA). Under the authority, direction, and control of the USD(I), the Director, DIA:

a. Assesses threats to U.S., allied, and coalition PNT and NAVWAR capabilities. Provides intelligence to CJCS, CCDRs, and Secretaries of the Military Departments to support NAVWAR activities. Coordinates with the Military Departments, the Joint Navigation Warfare Center (JNWC), and DOT&E, regarding PNT threat vignettes and scenarios to facilitate exercises, training, and testing.

b. Assesses the vulnerabilities of adversary PNT information systems and NAVWAR capabilities.

c. In coordination with the CJCS, the CCDRs, and the Secretaries of the Military Departments, ensures distribution of threat assessments and intelligence products to U.S. allies and coalition partners, as required to facilitate allied and coalition operations, exercises, and training.

2.8. DIRNSA/CHCSS. Under the authority, direction, and control of the USD(I), the DIRNSA/CHCSS:

a. Helps the DoD Components develop and manage PNT information assurance, including cryptography and integrated PNT device design.

b. Provides continuing electronic intelligence analysis of current and evolving systems and associated signals to the DoD Components to ensure correct identification and cataloguing of collected signals.

c. Leads DoD NAVWAR ES cooperative activities with U.S. allies and partners, in coordination with the DoD CIO, the Secretary of the Air Force, and the Director, NRO.

d. Develops a NAVWAR ES implementation plan to support the PNT and NAVWAR strategic plans referenced in Paragraph 2.1.c.

e. Develops procedures to protect PNT information and related cryptography pursuant to DoDD 5230.11 and in coordination with the DoD CIO, the CJCS, and the Secretaries of the Military Departments.

f. Implements allied and coalition partner cryptonet assignments to support allied and coalition operations, exercises, training, and R&D efforts as validated by the CJCS.

2.9. DIRECTOR, DEFENSE SECURITY COOPERATION AGENCY. Under the authority, direction, and control of the USD(P), the Director, Defense Security Cooperation Agency, ensures the CCDRs and the Security Cooperation Implementing Agencies receive periodic briefs on policy regarding the transfer of PNT and NAVWAR technology and capability to foreign militaries.

2.10. SECRETARIES OF THE MILITARY DEPARTMENTS The Secretaries of the Military Departments:

a. When an official acting under the authority, direction, and control of the Secretary of a Military Department is serving as MDA, ensure the MDA determines and confirms NAVWAR compliance at each acquisition milestone for all platforms and systems producing or using PNT information, in accordance with DoDI 5000.02 and Section 3 of this issuance.

b. When an official acting under the authority, direction, and control of the Secretary of a Military Department is serving as MDA, ensure that the MDA reviews test and evaluation plans to ensure they are sufficient to validate platform or system NAVWAR compliance standards.

c. Identify PNT contributions and NAVWAR environment assumptions, including all intentional and unintentional electromagnetic interference (including both Red and Blue electronic attack elements), and ensure they are addressed in applicable Military Service concepts, plans, and doctrine pursuant to and in accordance with this instruction. Coordinates with the other Military Departments, JNWC, and DIA, regarding PNT threat vignettes and scenarios to facilitate exercises, training, and testing. Collaborate with U.S. Strategic Command in the application of standardized NAVWAR threat conditions outlined in the PNT biennial assessment in determining relevant NAVWAR environments.

d. Designate a representative from each of their respective Departments to identify and advocate for PNT and NAVWAR requirements to establish and formalize joint NAVWAR requirements in accordance with CJCSI 3170.01I.

e. Conduct tests, training, and exercises in a NAVWAR environment with user-approved concepts of operation. Evaluate U.S. and allied NAVWAR capabilities versus assessed PNT and NAVWAR capabilities of potential adversaries.

f. Provide requirements to the Director, DIA, for assessment of:

(1) Threats to U.S., allied, and coalition PNT and NAVWAR capabilities.

(2) Vulnerabilities of adversary PNT information systems and NAVWAR capabilities.

g. Develop procedures to safeguard keyable PNT devices throughout their life cycle, including procedures for the destruction of security-controlled PNT devices, in coordination with the CJCS and the DIRNSA/CHCSS.

h. Ensure Security Classification Guides for all programs producing or using PNT information protect the specific PNT technologies and integration methods used.

i. Ensure all systems or platforms producing or using PNT information incorporate an open architecture design for the integration of multiple PNT sources to the maximum extent practicable in accordance with the Modular Open Systems Approach guidance contained in DoDI 5000.02 and in Section 805 of Public Law 114-328. PNT subsystems, if not designated as major system components, should have the attributes ascribed to major system components, as defined by Section 805 of Public Law 114-328 due to the need to address evolving technologies and threats.

j. Report to the DoD CIO the Service MDA determination regarding NAVWAR compliance for each platform or system under consideration for development or production following each acquisition milestone decision.

2.11. CJCS. The CJCS:

a. Ensures PNT and NAVWAR assumptions and considerations are addressed in joint concepts, plans, and doctrine pursuant to and in accordance with this instruction.

b. Ensures joint tests, training, and exercises are conducted in a NAVWAR environment.

c. Oversees allied and coalition partner crypto network assignment in support of allied and coalition operations, exercises, training, and R&D efforts in coordination with the DIRNSA/CHCSS.

d. Coordinates and formalizes joint PNT and NAVWAR requirements and capabilities across the DoD in accordance with CJCSI 3170.01I.

e. Ensures all requirements documents for systems and platforms producing or using PNT include the system survivability key performance parameter (KPP), as described in Paragraph 3.2.a.

2.12. CDRUSSTRATCOM. The CDRUSSTRATCOM:

a. Exercises command authority regarding the operational control of DoD space-based PNT assets.

b. Advocates for space-based PNT and joint NAVWAR capabilities.

- c. Supports Combatant Command joint training and planning related to NAVWAR operations; provides contingency NAVWAR support to other Combatant Commands; maintains the JNWC as the center of excellence for NAVWAR.
- d. Conducts allied and coalition partner cryptonet assignment in support of allied and coalition operations, exercises, training, and R&D efforts in coordination with the DIRNSA/CHCSS.
- e. As the Joint Proponent for space-based PNT and NAVWAR, integrates and coordinates space-based PNT and NAVWAR capabilities across the DoD and provides a biennial assessment of PNT and NAVWAR operational capabilities to the DoD CIO.
- f. Conducts PNT operational field assessments of DoD, adversary, and coalition NAVWAR capabilities and vulnerabilities to identify capability gaps, assess operational risk, and gain knowledge to enable PNT superiority in joint force and combined operations.
- g. In conjunction with the Secretaries of the Military Departments, provides requirements to the Director, DIA, for assessment of:
 - (1) Threats to U.S., allied, and coalition PNT and NAVWAR capabilities.
 - (2) Vulnerabilities of adversary PNT information systems and NAVWAR capabilities.
- h. Coordinates PNT- and NAVWAR-related tests, training, and exercises with the appropriate defense and federal agencies to ensure impact to other PNT users is minimized outside the boundaries of the test, training, and exercise area.
- i. Supports the United States Northern Command in assessing PNT- and NAVWAR-related threat effects to U.S. critical infrastructure.
- j. Collaborates with the Military Services in the application of Standardized NAVWAR Threat Conditions outlined in the biennial DoD PNT Assessment in determining relevant condition levels to enable evaluation and testing of PNT capabilities.

2.13. COMMANDER, UNITED STATES CYBER COMMAND (CDRUSCYBERCOM).

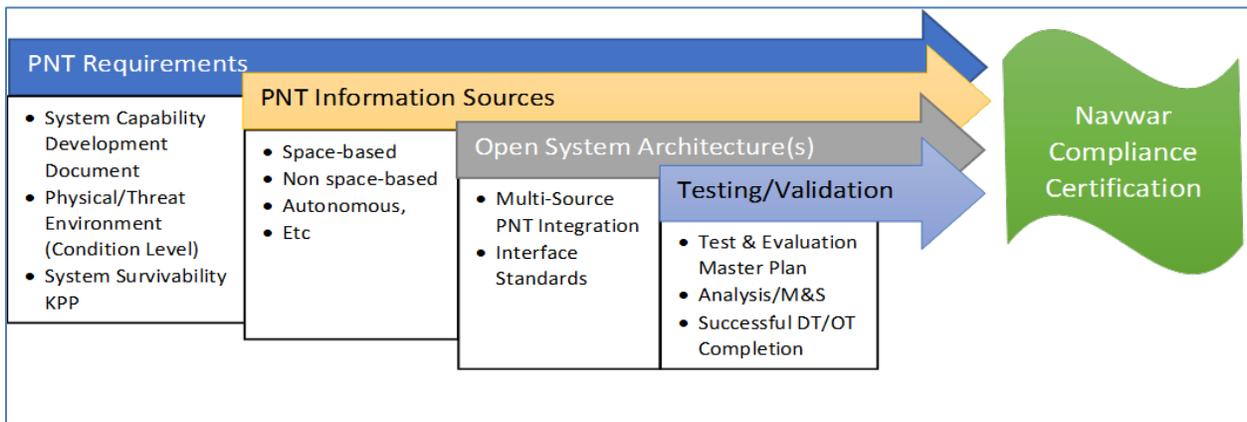
The CDRUSCYBERCOM:

- a. Advocates for PNT and NAVWAR capabilities to support Department of Defense Information Network (DODIN) operations.
- b. Ensures the necessary actions are taken to secure and defend DoDIN operations that could be impacted by any hostile or malicious attack against a DoDIN PNT asset.
- c. In coordination with Commander, USSTRATCOM, and other Combatant Commanders as required, ensures cyber capabilities are developed, realistically tested, and made available in support of Joint Force NAVWAR mission needs.

SECTION 3: NAVWAR COMPLIANCE PROCEDURES

3.1. DISCUSSION. The purpose of the following NAVWAR compliance procedures is to prescribe clearly the steps that must be taken for any program or system that uses PNT information to determine successfully whether they are NAVWAR compliant. A system is NAVWAR compliant if it continues to provide trusted PNT information over the time period required by a specific mission at the level of accuracy required by the mission in the expected physical, electromagnetic, and cyber environment. Figure 1 provides a pictorial view of the components of the NAVWAR compliance process.

Figure 1. NAVWAR Compliance Process Components



3.2. CAPABILITY DEVELOPMENT AND SYSTEM INTEGRATION.

a. Each program or system producing or using PNT information must incorporate the following system survivability KPPs in its capability development document: The PNT capabilities employed by the program or system must maintain tactical resiliency and continue to provide trusted PNT information at the level of accuracy required by the mission in the expected physical, electromagnetic, and cyber environment for a minimum of “x” period of time (the “x” being the period of time the platform or system needs accurate PNT to successfully complete its mission in this expected NAVWAR environment).

b. Each program or system will determine the worst-case NAVWAR environment within which the platform or system will be required to operate. Table 1 may be used as a model for this determination. Condition levels should be described in sufficient detail to enable evaluation and testing of PNT capabilities planned for use by DoD platforms or systems to operate successfully and demonstrate tactical resiliency within required NAVWAR and physical environments. These condition levels should be used in conjunction with standardized threat levels during the development and operational testing processes, ranging from low to high threat levels.

c. Determine what mix of PNT capabilities, integrated using a Modular Open System Approach to the maximum extent possible, is necessary to meet the KPP defined in the capability development document in the worst-case environment.

Table 1. Notional PNT Conditions and Capabilities for NAVWAR Compliance

Level	Condition	PNT Capability
0	Low - mission accomplished without precision PNT	No Special PNT Protection - Commercial GPS SPS without authentication, unkeyed military GPS receivers in SPS mode, any GNSS Open Service signals, or other PNT sources not previously considered and accepted for use by the DoD
1	Moderate - mission accomplished at slightly degraded level (slower pace, reduced weapon selection, some collateral damage) without precision PNT	Limited PNT Access –Keyed P(Y) and M-Code equipment, other trusted signals (with authentication), or accepted signals of opportunity which may be available
2	High - mission accomplished at degraded level (slower pace, limited selection of precision weapons, collateral damage, fratricide) without precision PNT	Assured PNT in Challenged Environments - Keyed M-Code or P(Y)-Code receivers with self-contained PNT source(s), authorized foreign GNSS through MOA with DoD, or approved terrestrial RF navigation signals
3	Extremely High - mission accomplished at an extremely degraded level (very slow pace, no use of precision weapons, imminent danger of collateral damage/ fratricide) without precision PNT	Assured PNT in Severe Environments - Keyed Global Positioning System (GPS) M-Code or P(Y)-Code receivers [assumes use of assistive technology and AJ augmentations] or self-contained PNT source(s) operating within its/their effective performance envelope(s)

3.3. DEVELOPMENTAL AND OPERATIONAL TEST AND EVALUATION.

a. Review system test and evaluation plans for programs producing or using PNT information to ensure they are sufficient to validate platform or system NAVWAR compliance assessment. The USD(R&E) will conduct the review of test and evaluation plans of acquisition programs for which the USD(A&S) is the MDA, and the responsible Service authority will conduct the review of test and evaluation plans of acquisition programs for which the MDA is at the Service level.

b. Conduct system test and evaluation (e.g., real-world test; modeling and simulation; empirical analysis) sufficient to validate that all systems or platforms producing or using PNT information meet the system survivability KPP referred to in Paragraph 3.2.a.

3.4. MODIFICATION OF FIELDDED PNT CAPABILITIES AND AQUISITIONS OUTSIDE THE DEFENSE ACQUISITION SYSTEM.

Any platform or system undergoing PNT capability modification or upgrade, or acquired outside the Defense Acquisition System, is subject to Paragraphs 1.2.d. and 1.2.e. Capability developers and DoD Components must consider and demonstrate completion of equivalent activities to those described in Paragraphs 3.2. and 3.3. to ensure NAVWAR compliance. The Component Acquisition Executive or DoD

Component chief information officer must notify the DoD PNT Executive Management Board of NAVWAR compliance. The notification template is contained in DoDM O-4650.11. The notification must address the requirements of either Paragraph 1.2.d. or 1.2.e. in the following manner:

a. Combat, Combat Support, and Combat Service Support. The system is NAVWAR compliant if the PNT capabilities employed by the program or system are capable of providing trusted PNT information over the time periods and at the level of accuracy required for all missions in which it is used in the expected physical, electromagnetic, and cyber environment.

b. Non-Combat Operations. In the event the PNT capability incorporates civil, commercial, or foreign sources, the system is NAVWAR compliant if the PNT capability provides trusted PNT information over the time periods and at the level of accuracy required for all missions in which it is used in the expected physical, electromagnetic, and cyber environment.

GLOSSARY

G.1. ACRONYMS.

CCDR	Combatant Commander
CDRUSCYBERCOM	Commander, United States Cyber Command
CDRUSSTRATCOM	Commander, United States Strategic Command
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
crypto	cryptographic
DIA	Defense Intelligence Agency
DIRNSA/CHCSS	Director, National Security Agency/Chief, Central Security Service
DoD CIO	DoD Chief Information Officer
DoDD	DoD directive
DoDI	DoD instruction
DoDIN	Department of Defense Information Network
DOT&E	Director of Operational Test and Evaluation
ES	electronic warfare support
JNWC	Joint Navigation Warfare Center
KPP	key performance parameter
MDA	Milestone Decision Authority
NAVWAR	navigation warfare
NRO	National Reconnaissance Office
PNT	positioning, navigation, and timing
R&D	research and development
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(I)	Under Secretary for Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy
USD(R&E)	Under Secretary of Defense for Research and Engineering

G.2. DEFINITIONS. Unless otherwise noted, these terms and their definitions are for the purposes of this issuance.

combat service support. Defined in the DoD Dictionary of Military and Associated Terms.

combat support. Defined in the DoD Dictionary of Military and Associated Terms.

ES. Defined in the DoD Dictionary of Military and Associated Terms.

integrated PNT. A combination of multiple PNT sources, NAVWAR, and joint and Service doctrine meant to provide assured PNT information to military users operating in a NAVWAR environment.

NAVWAR. Defined in the DoD Dictionary of Military and Associated Terms.

NAVWAR compliance. A PNT system that continues to provide trusted PNT information over the time period required by a specific mission at the level of accuracy required by the mission in the expected physical, electromagnetic, and cyber environment.

NAVWAR environment. The expected physical, electromagnetic, and cyber conditions in which a PNT system operates.

strategic plan. A strategy that aligns requirements with timelines for specific materiel and non-materiel solutions to provide a means to establish priorities and forecast technology developments, as well as a framework to coordinate efforts.

trusted PNT information. PNT information that can be continuously verified or validated.

REFERENCES

- Chairman of the Joint Chiefs of Staff Instruction 3170.01I, “Joint Capabilities Integration and Development System (JCIDS),” January 23, 2015
- Chairman of the Joint Chiefs of Staff Instruction 6130.01F, “Master Positioning, Navigation, and Timing Plan,” September 30, 2016 ¹
- DoD Directive 3100.10, “Space Policy,” October 18, 2012, as amended
- DoD Directive 4650.05, “Positioning, Navigation, and Timing (PNT),” June 9, 2016
- 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 Instruction 5000.02, “Operation of the Defense Acquisition System,” January 7, 2015, as amended
- DoD Instruction 2040.02, “International Transfers of Technology, Articles, and Services,” March 27, 2014, as amended
- DoD Instruction 4650.06, “Positioning, Navigation, and Timing (PNT) Management,” June 16, 2016
- DoD Instruction 8500.01, “Cybersecurity,” March 14, 2014
- DoD Manual O-4650.11, “Positioning, Navigation, and Timing (PNT) Security,” May 26, 2017, as amended
- Intelligence Community Directive 115, “Intelligence Community Capability Requirements Process,” December 21, 2012
- Office of the Chairman of the Joint Chiefs of Staff, “DoD Dictionary of Military and Associated Terms,” current edition
- Public Law 114–328, Section 805, “National Defense Authorization Act for Fiscal Year 2017,” December 23, 2016

¹ Releasability is limited (not approved for public release). This instruction is approved for .mil/.gov access only on NIPRNet. DoD Components (to include the Combatant Commands) and other federal agencies may obtain copies of this instruction through controlled access at http://www.dtic.mil/cjcs_directives/. DoD Components may also obtain access via the SIPRNet Directives Electronic Library Website.