Department of Defense
INSTRUCTION

NUMBER 4650.08
February 5, 2015

DoD CIO

SUBJECT: Positioning, Navigation, and Timing (PNT) and Navigation Warfare (Navwar)

References: See Enclosure 1

1. PURPOSE. This instruction:

a. Establishes policy and assigns responsibilities in accordance with the authority in DoD Directive (DoDD) 5144.02 (Reference (a)) for integrating PNT and Navwar across the DoD pursuant to DoDD 4650.05 (Reference (b)), and DoD Instruction (DoDI) 5000.02 (Reference (c)).

b. Establishes policy and assigns responsibilities for the security of PNT information related to the development, acquisition, and operational use of PNT information sources and PNT information-dependent systems pursuant to References (a) through (c) and DoDD 8500.01E (Reference (d)).

c. Implements PNT and Navwar policy pursuant to Reference (b).

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

3. POLICY. It is DoD policy that:

a. U.S. and allied forces will effectively employ Navwar capabilities to ensure a PNT advantage in support of military operations.

b. Programs providing PNT capabilities or using PNT information must be Navwar compliant and will report Navwar compliance to the Milestone Decision Authority (MDA) at each acquisition program milestone in accordance with References (a) and (c).

c. Navwar compliance, 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.

d. Reliance on non DoD-approved civil, commercial, or foreign sources as the primary means of obtaining PNT information for combat or combat support operations is **not** authorized.

e. Reliance on civil, commercial, or foreign sources as the primary means of obtaining PNT information for combat service support operations is authorized, subject to the level of PNT integrity required.

f. Integration of PNT information from an unprotected external source is authorized pursuant to this instruction. The unprotected external source contribution to the integrated PNT information will be defined in the PNT user equipment architecture guidelines.

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

h. Access to DoD PNT services by U.S. federal civil agencies and foreign government entities may be authorized as described in Enclosure 2. Access must be approved consistent with applicable U.S. laws, regulations, and DoD policy, including disclosures in accordance with DoDD 5230.11 (Reference (e)) and exports in accordance with DoDI 2040.02 (Reference (f)).

4. RESPONSIBILITIES. See Enclosure 2.

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

6. EFFECTIVE DATE. This instruction is effective February 5, 2015.

Terry A. Halvorsen
Acting DoD Chief Information Officer

Enclosures
1. References
2. Responsibilities

Glossary

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014
(b) DoD Directive 4650.05, "Positioning, Navigation, and Timing (PNT)," February 19, 2008
(c) DoD Instruction 5000.02, "Operation of the Defense Acquisition System," January 7, 2015
(d) DoD Instruction 8500.01, "Cybersecurity" March 14, 2014
(e) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992
(f) DoD Instruction 2040.02, "International Transfers of Technology, Articles, and Services," July 10, 2008
(g) DoD Directive 3100.10, "Space Policy," October 18, 2012
(h) DoD Instruction 4650.06, "DoD Positioning, Navigation, and Timing (PNT) Executive Committee and Working Groups," November 24, 2009
(i) DoD Global Positioning System (GPS) Security Policy, April 4, 2006[1]
(j) Intelligence Community Directive 115, "Intelligence Community Capability Requirements Process," December 21, 2012
(k) Chairman of the Joint Chiefs of Staff Instruction 3170.01H, "Joint Capabilities Integration and Development System," January 10, 2012
(l) Presidential Policy Directive 21, "Critical Infrastructure Security and Resilience," February 12, 2013
(m) Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," current edition

[1] Document available by request from DoD CIO, 6000 Defense Pentagon, Washington, DC 20301-6000 Attn: Director, Space Programs and Policies

ENCLOSURE 2

RESPONSIBILITIES

1. DoD CIO. The DoD CIO:

a. Leads the development and coordination of DoD strategy and policy related to PNT as part of the DoD Information Enterprise in accordance with Reference (a) and DoDD 3100.01 (Reference (g)).

b. In accordance with References (a), (c), and DoDI 4650.06 (Reference (h)), develops and oversees implementation and coordination of PNT and Navwar policy via the DoD PNT Executive Committee.

c. Oversees the development and publication of DoD PNT and Navwar strategic plans.

d. Develops and publishes procedures for determining Navwar policy compliance and assessing Navwar capabilities for programs using or providing PNT information.

e. Develops and maintains a DoD issuance for PNT security procedures, in coordination with the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) and other DoD PNT Executive Committee members, that incorporates the tenets of Reference (d) and updates and replaces the DoD Global Positioning System (GPS) Security Policy (Reference (i)).

f. Develops and publishes, with Army participation as lead component for Assured PNT, security and performance certification procedures to ensure PNT devices incorporate the required security architecture and design considerations to protect critical technology and to assess the applicable PNT integrity level(s).

g. Develops and publishes guidance for PNT and Navwar international cooperation, to include policy governing assignment of cryptographic (crypto) networks, in support of allied and coalition operations, exercises, training, and research and development (R&D) efforts, pursuant to Reference (a) and in coordination with the Under Secretary of Defense for Policy (USD(P)), the USD(AT&L), CJCS, Secretaries of the Military Departments, Commander, United States Strategic Command (CDRUSSTRATCOM), and the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS).

2. USD(AT&L). The USD(AT&L):

a. Incorporates DoD CIO guidance for PNT and Navwar into R&D programs and acquisition programs for systems that use or provide PNT information.

b. Provides oversight of acquisition related PNT and system level architecture issues.

c. Ensures that acquisition programs are Navwar compliant in accordance with this instruction.

d. Ensures all DoD systems using or providing PNT information are tested in a Navwar environment in coordination with Director of Operational Test and Evaluation (DOT&E) and DoD CIO.

3. DOT&E. The DOT&E coordinates with the USD(AT&L) and DoD CIO to ensure that all DoD systems using or providing PNT information are tested in a Navwar environment.

4. DIRECTOR, NATIONAL RECONNAISSANCE OFFICE (NRO). Under the authority, direction, and control of the Under Secretary of Defense for Intelligence (USD(I)), the Director, NRO:

a. Documents Navwar electronic support (ES) requirements pursuant to Intelligence Community Directive 115 (Reference (j)) or CJCS Instruction 3170.01H (Reference (k)) and in coordination with the CJCS, Combatant Commanders (CCDRs), Secretaries of the Military Departments, and the DIRNSA/CHCSS.

b. Provides technical assistance and subject matter expertise to support efforts of the Secretaries of the Military Departments to develop and field Navwar ES-related capabilities and associated doctrine.

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

a. Assesses and reports on threats to U.S., allied, and coalition PNT and Navwar capabilities. Provides intelligence products to United States Strategic Command to support activities of the Joint Navigation Warfare Center (JNWC).

b. Assesses and reports on the vulnerabilities of adversary PNT information systems and Navwar capabilities.

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

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

a. Provides assistance in the development and management of 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 ensure correct identification and cataloguing of collected signals.

c. Leads DoD Navwar ES cooperative activities with U.S. allies, 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 1c of this enclosure.

e. Establishes procedures to protect PNT information and related cryptography pursuant to Reference (e) and in coordination with the DoD CIO, CJCS, and the Secretaries of the Military Departments.

f. Facilitates allied and coalition partner assignment of cryptonets in support of allied and coalition operations, exercises, training, and R&D efforts as validated by the CJCS.

7. DIRECTOR, DEFENSE SECURITY COOPERATION AGENCY (DSCA). Under the authority, direction, and control of the USD(P), the Director, DSCA, ensures that policy regarding the transfer of PNT and Navwar technology and capability to foreign militaries is periodically briefed to the CCDRs and the implementing agencies.

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

a. Identify PNT contributions and Navwar environment assumptions and ensure they are addressed in applicable Service concepts, plans, and doctrine pursuant to and in accordance with this instruction.

b. Establish a Service proponent to identify and advocate for PNT and Navwar requirements through CDRUSSTRATCOM to the Joint Staff to establish and formalize joint Navwar requirements in accordance with Reference (k).

c. Conduct tests, training, and exercises in a Navwar environment and include evaluation of Navwar capability versus assessed PNT and Navwar capabilities of potential adversaries.

d. Provide an assessment of Navwar compliance to the MDA at each acquisition milestone for programs using or providing PNT information.

e. Provide requirements to the Director, DIA, for assessment of threats to U.S., allied, and coalition PNT and Navwar capabilities.

f. Provide requirements to the Director, DIA, for assessment of the 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 DIRNSA/CHCSS.

h. Implement security and performance certification processes in accordance with CIO procedures to validate PNT devices to the required level of PNT integrity.

9. SECRETARY OF THE ARMY. In addition to the responsibilities in section 8 of this enclosure, the Secretary of the Army:

a. Assists the DoD CIO in the development of security and performance certification procedures for PNT devices.

b. Provides detailed PNT device guidelines and architecture documentation.

c. Provides detailed guidance on PNT assurance levels, to include assessment methodology.

10. CJCS. The CJCS:

a. Ensures that PNT and Navwar assumptions and considerations are addressed in joint concepts, plans, and doctrine pursuant to and in accordance with the policy and definitions in this instruction.

b. Ensures joint tests, training, and exercises are conducted in a Navwar environment. Includes an evaluation of Navwar compliance and capability versus assessed PNT and Navwar capabilities of potential adversaries in these events.

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 DIRNSA/CHCSS.

d. Coordinates and formalizes joint PNT and Navwar requirements and capabilities across the DoD in accordance with Reference (k).

11. CDRUSSTRATCOM. The CDRUSSTRATCOM:

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

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

c. Integrates and coordinates PNT and Navwar requirements and capabilities across the DoD and maintains the JNWC as the center of excellence for Navwar.

d. Conducts PNT operational field assessments of DoD, adversary, and coalition Navwar capabilities and vulnerabilities to identify capability gaps, assess operational risk, and provide knowledge to enable PNT superiority in joint force and combined operations. Provide an annual assessment of Navwar operational capabilities to the DoD CIO.

e. Ensures necessary budget resources are prioritized and allocated to maintain resources for the JNWC.

f. Provides requirements to the Director, DIA, for assessment of threats to U.S., allied, and coalition PNT and Navwar capabilities.

g. Provides requirements to the Director, DIA, for assessment of the vulnerabilities of adversary PNT information systems and Navwar capabilities.

h. Coordinates PNT and Navwar related tests, training, and exercises with the appropriate military and civil agencies to ensure impact to other PNT users is minimized outside the boundaries of the test, training, and exercise area.

i. Supports Combatant Command joint training and planning related to Navwar, and provides contingency Navwar support.

j. In coordination with the Commanders, United States Pacific Command and United States Northern Command, assesses PNT and Navwar related threat effects to U.S. critical infrastructure pursuant to Presidential Policy Directive 21 (Reference (l)).

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

CCDR	Combatant Commander
CDRUSSTRATCOM	Commander, United States Strategic Command
CJCS	Chairman of the Joint Chiefs of Staff
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
DOT&E	Director of Operational Test and Evaluation
DSCA	Defense Security Cooperation Agency
ES	electronic support
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
JNWC	Joint Navigation Warfare Center
MDA	Milestone Decision Authority
Navwar	navigation warfare
NRO	National Reconnaissance Office
PNT	positioning, navigation, and timing
R&D	research and development
RF	radio frequency
SPS	standard positioning service
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I)	Under Secretary for Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy

PART II. DEFINITIONS

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

combat service support. Defined in Joint Publication 1-02 (Reference (m)).

combat support. Defined in Reference (m).

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. Integrated PNT is Navwar capable and compliant.

Navwar. Defined in Reference (m).

Navwar compliance. Employment of trusted PNT sources, as necessary, to provide required levels of PNT assurance and integrity across the PNT enterprise-wide architecture.

Navwar environment. A test, exercise, or operation in which the primary source of PNT information necessary for system operation to meet program specifications is unavailable or inefficacious due to blue, red, or environmental interference and use of alternative material or non-material solutions is required to maintain specified performance.

PNT assurance. The methods and capabilities employed to assure warfighter access to PNT information at appropriate levels of PNT integrity where and when required.

PNT integrity. A quality and dependability measure of PNT Information. PNT integrity is maintained if the PNT Information retains the accuracy, precision, and availability expected from the PNT source over the time period required by a specific mission. Use of a graduated scale defines the ability of PNT sources to provide the necessary PNT integrity to support specific mission requirements. Levels of PNT integrity will vary depending on the extent to which PNT information is derived from trusted PNT sources.

high integrity PNT (Level 3). Derived from keyed GPS M-Code or P(Y)-Code receivers or self-contained PNT sources (inertial, clock, electro-optical) operating within their effective performance envelopes.

medium-high integrity PNT (Level 2). Derived from keyed GPS M-Code or P(Y)-Code receivers coupled with self-contained PNT sources (inertial, clock, electro-optical), authorized foreign global navigation satellite system (GNSS) signals made available through international agreement with the DoD, or from previously defined terrestrial radio frequency (RF) navigation system signals.

medium integrity PNT (Level 1). Derived from GPS standard positioning service (SPS) signals (with integrity authentication provisions), from trusted foreign GNSS open service signals (with integrity authentication provisions), from previously defined civil terrestrial RF navigation system signals, or from considered and accepted signals of opportunity which may be available.

low integrity PNT (Level 0). Derived from commercial GPS SPS receivers without integrity authentication provisions, from unkeyed military GPS receivers operating in the SPS mode, from

all GNSS open service signals, or from other PNT sources not previously considered and accepted for use by the DoD.

strategic plan. 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 source. A controlled source of PNT information that can be continuously verified or validated for PNT integrity.