CJCSI 6130.01E
1 May 2013

2013 CJCS MASTER POSITIONING, NAVIGATION, AND TIMING PLAN (MPNTP)

JOINT STAFF
WASHINGTON, D.C. 20318

(INTENTIONALLY BLANK)

CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J-6 CJCSI 6130.01E
DISTRIBUTION: A, B, C 1 May 2013

2013 CJCS MASTER POSITIONING, NAVIGATION, AND TIMING PLAN (MPNTP)

References: See Enclosure O.

1. Purpose

a. This instruction provides overarching guidance and procedures for the planning, use, and management of the Department of Defense (DoD) positioning, navigation, and timing (PNT) systems either owned or contracted for use to meet operational warfighter requirements. This instruction reflects the policy and directions contained in referenced documents listed in Enclosure O and implements the Chairman of the Joint Chiefs of Staff (CJCS) joint systems responsibilities.

b. Service and Defense agency PNT requirements are validated in accordance with CJCSI 3170.01H and this document. The resulting validated programs become the basis for Service and Defense agency PNT programming and program objective memorandum (POM) submissions to the Office of the Secretary of Defense (OSD). This master plan also serves as the primary DoD input to the Department of Defense, Department of Transportation (DoT) and Department of Homeland Security Federal Radionavigation Plan (FRP) (see Enclosure O, reference a), and appropriate North Atlantic Treaty Organization (NATO), bilateral, and multilateral plans.

2. Cancellation. CJCSI 6130.01D, 13 April 2007, "2007 CJCS Master Positioning, Navigation and Timing Plan," is hereby superseded by this document.

3. Applicability. This instruction applies to the Joint Staff, combatant commands (CCMDs), Services, Defense agencies, Defense Research Agencies, and other agencies and organizations that develop, use or plan to use DoD PNT to include the Global Positioning System (GPS). A GPS user is defined as any entity that uses GPS User Equipment (UE), whether the Department of Defense owned or contracted for use. A GPS Precise Positioning Service (PPS) user is

one who implements the elements of the GPS security architecture, including cryptography (crypto), Selective Availability (SA), and Anti-Spoofing (AS) via P(Y)-code or M-code generation to provide Position, Velocity, and Timing (PVT) data. Though not directive in nature to our allies, this instruction acts as guidance for U.S. allies.

4. Policy. DoD policy requires a consistent and logical integration of secure PNT systems. This includes integrating the data, schedules, programs, plans, and responsibilities for PNT systems among the Joint Staff, CCMDs, Services, and other DoD agencies; and between this instruction and the FRP.

5. Definitions. Refer to the Glossary, Enclosure GL.

6. Responsibilities. See Enclosure A, paragraph 3; and Enclosure D, paragraph 4.

7. Review Procedures. This instruction will be reviewed annually and revised as necessary, normally biennially. Recommendations for changes from the CCMDs should be submitted to the Director for C4 Systems, J-6, Joint Staff, Washington, DC 20318-6000. Service and Defense agency recommendations should be submitted through the following addressees:

a. U.S. Army. HQDA CIO/G6, Attn: SAIS AON, 700 Army Pentagon, Washington, DC 20310-0700.

b. U.S. Navy. Chief of Naval Operations (CNO-N2/N6E), 2000 Navy Pentagon Washington, DC 20350-2000.

c. U.S. Air Force. Director of Operational Capability Requirements, HQ USAF, Space Requirements Division (HQ USAF/A5R), 1480 Air Force Pentagon, Washington, DC 20330-1480.

d. U.S. Marine Corps. Commandant of the Marine Corps, Attn: HQMC (Code C4 CS), 3000 Marine Corps Pentagon, Room 1D247, Washington, DC 20350-3000.

e. NSA. Director, National Security Agency, Attn: IA Director, 9800 Savage Road, Ft. George G. Meade, MD 20755-6710.

f. DISA. Director, Defense Information Systems Agency, Attn: DNSO, D311 DISN Transport Operations Branch, 701 South Courthouse Road, Arlington, VA 22204-2199.

g. NGA. Director, NGA, Attn: NGA Springfield, 7500 GEOINT Drive, Springfield, VA, 22150-7500.

FOR OFFICIAL USE ONLY

h. USNO. Superintendent, U.S. Naval Observatory, 3450 Massachusetts Ave NW, Washington, DC 20392-5421.

8. Summary of Changes. This instruction updates the Department of Defense's PNT plans and policy.

9. Releasability. NOT FOR PUBLIC RELEASE. This directive is approved for limited release. DoD Components (to include the combatant commands) and other Federal agencies may obtain copies of this directive through controlled Internet access from the CJCS Directives Electronic Library at http://www.dtic.mil/cjcs_directives. Joint Staff activities may also access or obtain copies of this directive from the JS-DSE.

10. Effective Date. This instruction is effective immediately.

For the Chairman of the Joint Chiefs of Staff:

CURTIS M. SCAPARROTTI,
Lieutenant General, U.S. Army
Director, Joint Staff

Enclosures:

A – Positioning, Navigation, and Timing (PNT) Policy
B – PNT Requirements
C – PNT System Architecture
D – GPS: Operations, Security Policy and Responsibilities
E – Navigation Warfare (NAVWAR)
F – GPS User Equipment (UE) Acquisition Policy
G – PNT Capabilities, Sciences and Technologies
H – Control of PNT in Times of Tension and War
I – Geospatial Information and Services
J – Precise Time and Time Interval (PTTI)
K – Waiver Request Process Flow Chart
L – PNT Waiver Request Format Example
M – PNT Waiver Request Approval
N – PNT PPS Waiver Denial
O – References
GL - Glossary

FOR OFFICIAL USE ONLY

(INTENTIONALLY BLANK)

DISTRIBUTION

Distribution A, B, and C plus the following:

	Copies
Secretary of State	2
Secretary of Transportation	2
Secretary of Homeland Security	2
Secretary of Commerce	2
Commandant of the Coast Guard	2
Under Secretary of Defense for Policy	2
Under Secretary of Defense for Intelligence	2
Under Secretary of Defense for Acquisition, Technology and Logistics	2
Department of Defense Chief Information Officer (DoD CIO)	2
Secretary Air Force	2
Administrator of the Federal Aviation Administration	2
Director, National Security Agency	2
Director, Defense Advanced Research Projects Agency	2
Director, National Geospatial-Intelligence Agency	1
Director, National Reconnaissance Office	2
Administrator, National Aeronautics and Space Administration	2
Administrator, Defense Technical Information Center	1
President, National Defense University	1
Commandant, Armed Forces Staff College	2
Director, Office of Management and Budget	1
U.S. Delegate to the Military Committee, NATO	2
Commander, U.S. Cyber Command	1
Commander, Joint Information Operations Center	1
Commander, United States Strategic Command	4
Commander, U.S. Pacific Command	1
Commander, U.S. Central Command	1
Commander, U.S. European Command	1
Commander, U.S. Southern Command	1
Commander, U.S. Northern Command	1
Commander, U.S. Transportation Command	1
Commander, U.S. Africa Command	1
Commander, Naval Meteorology & Oceanography Command	1
Air Force Space Command	4
Air Force Space and Missile Systems Center	2
Joint Functional Component Command for Space	2
Naval Space Command	2
U.S. Army Space and Missile Defense Command/Army Strategic Forces	2
Air Force Operational Test and Evaluation Center	2
National Executive Committee for Space-Based PNT	2
National Coordination Office for Space-Based PNT	2
Deputy Under Secretary of the Air Force (Space Program)/Executive Agent for Space Staff	2
Army Strategic Command	1
Army Test and Evaluation Center	2
Fleet Cyber Command	1
Navy Operational Test and Evaluation Force	2
Space and Naval Warfare Systems Command	2

FOR OFFICIAL USE ONLY

46th Test Group/746th Test Squadron 2
Joint Navigation Warfare Center..... 2
U.S. Naval Observatory, Washington, DC 2
U.S. Naval Observatory, Flagstaff Station, AZ 2
U.S. Naval Observatory, Schriever AFB, CO 2
Defense Threat Reduction Agency..... 2
Defense Security Cooperation Agency..... 2
Defense Information Systems Agency..... 2

FOR OFFICIAL USE ONLY

TABLE OF CONTENTS

Page

ENCLOSURE A - POSITIONING, NAVIGATION, AND TIMING (PNT) POLICY ..A-1

ENCLOSURE B - PNT REQUIREMENTS B-1

ENCLOSURE C - PNT SYSTEM ARCHITECTURE C-1

ENCLOSURE D - GPS: OPERATIONS, SECURITY POLICY AND RESPONSIBILITIES D-1

ENCLOSURE E - NAVIGATION WARFARE (NAVWAR) E-1

ENCLOSURE F - GPS UE ACQUISITION POLICY F-1

ENCLOSURE G - PNT CAPABILITIES, SCIENCES, AND TECHNOLOGIES.... G-1

ENCLOSURE H - CONTROL OF PNT IN TIMES OF TENSION OR WAR..... H-1

ENCLOSURE I - GEOSPATIAL INFORMATION AND SERVICES.....I-1

ENCLOSURE J - PRECISE TIME AND TIME INTERVAL (PTTI) J-1

ENCLOSURE K – WAIVER REQUEST PROCESS FLOW CHART K-1

ENCLOSURE L – PNT WAIVER REQUEST FORMAT EXAMPLE L-1

ENCLOSURE M – PNT WAIVER REQUEST ENDORSEMENT..... M-1

ENCLOSURE N – PNT WAIVER REQUEST ENDORSEMENT DENIAL N-1

ENCLOSURE O – REFERENCES O-1

ENCLOSURE GL –GLOSSARY GL-1

FOR OFFICIAL USE ONLY

(INTENTIONALLY BLANK)

FOR OFFICIAL USE ONLY

ENCLOSURE A

POSITIONING, NAVIGATION AND TIMING POLICY

1. Scope. This instruction documents DoD policy, requirements, acquisition planning, operational use and sustainment of PNT systems.

a. This plan does not cover every possible topic related to PNT. For example, it makes no detailed reference to visual navigation (e.g., map and compass), nor to such topics as use of navigation charts or notices to mariners.

b. This plan uses the term PNT to apply to both the end use of Positioning, Velocity, and Timing (PVT) information, as well as to the various systems that generate PVT information.

2. Summary of Key PNT Policies

a. General Military Policy. In conducting military operations described in Joint Vision 2020, it is essential that PNT services be available with the highest possible confidence. These services must meet or exceed mission requirements, and in some cases must anticipate requirements well beyond the normal DoD Planning, Programming Budgeting and Execution (PPBE) and Future Years Defense Program (FYDP) process. In order to meet these mission requirements, information that refers to a position on the Earth, in the Earth's atmosphere, or in space must indicate that position in terms of the standard geospatial reference frame defined by the World Geodetic System 1984 (WGS-84) as provided by the National Geospatial-Intelligence Agency (NGA). Any information that makes reference to time must be able to provide that time in terms of the standard temporal reference defined by Coordinated Universal Time (UTC) as maintained by the US Naval Observatory (USNO) Master Clock.

(1) Only DoD-approved PNT systems will be used for combat, combat support and combat service support operations. These DoD-approved PNT systems currently include Inertial Navigation Systems (INS) and properly keyed GPS PPS. For more detailed descriptions of combat, combat support and combat service support elements, see Enclosure C.

(2) DoD PNT users (e.g., ships, aircraft, etc.) may use civil PNT systems in *peacetime* where the use of civil systems does not jeopardize the ability to carry out peacetime military training or peacetime operations (e.g., civil personnel rescue, disaster relief, etc.). If civil PNT systems are used by the DoD in peacetime, they shall also meet International Maritime Organization (IMO), International Civil Aviation Organization (ICAO), Federal Aviation Administration (FAA) or DoD specifications. See Enclosure B for more details.

FOR OFFICIAL USE ONLY

(3) Exceptions and waiver requirements to (1) and (2) above can be found in this instruction, Enclosure D.

b. Survivability Needs. PNT systems should be designed to be as survivable and robust as the forces and weapon systems they are designed to support. The Services shall use physical security, hardening, electronic protection (EP) mechanisms, and other measures to protect cryptography, ensure the availability of PNT services to the U.S. and its allies, and retain capability to deny hostile use of PNT information when necessary.

c. Continuity. Current PNT systems must be sustained until follow-on systems have been validated for operational use.

d. Need for Periodic Reviews. Under the leadership of the Joint Requirements Oversight Council (JROC) and the DoD PNT Executive Committee (EXCOM), the Department of Defense will use the Joint Capabilities Integration and Development System (JCIDS) and the PNT Science and Technology (S&T) community to conduct periodic reviews of emerging PNT technologies to determine their ability to meet operational requirements. The JS represents the interests of the joint warfighter, on behalf of the CJCS, in each of these activities. The Department of Defense will use the PNT architecture and Solutions Recommendations Phase of the JCIDS process.

e. Global Positioning System (GPS). GPS is, and will continue to be, the primary source of PNT information for the Department of Defense. All DoD combatant users must acquire, train with, and use GPS PPS systems in accordance with the DoD GPS Security Policy document (see Enclosure O, reference b) and this instruction. The National Defense Authorization Act (NDAA) for FY 1994 (Public Law 103-160), as amended by NDAA for FY 2005 (Public Law 108-375), mandates that "*after September 30, 2007, funds may not be obligated to modify or procure any Department of Defense aircraft, ship, armored vehicle, or indirect-fire weapon system that is not equipped with a Global Positioning System receiver.*" Additionally, NDAA for FY 2011 (Public Law 111-383) mandates that 'none of the funds authorized to be appropriated…for the Department of Defense may be obligated or expended to purchase user equipment for the Global Positioning System during fiscal years after fiscal year 2017 unless the equipment is capable of receiving the military code (commonly known as the M-Code). The DoD GPS Security Policy and this instruction further mandate those systems/platforms be equipped with approved PPS devices. PPS is the encrypted GPS service provided on both the GPS L1 and L2 frequencies. PPS uses encrypted signals on the two separate frequencies to provide authorized users enhanced accuracy and Anti-Spoofing (A/S) protection against deliberate radiation, re-radiation, or alteration of electromagnetic energy intended to convey misleading information. An enhanced signal (M-code), separate from the current P(Y)-coded signal, has

FOR OFFICIAL USE ONLY

been developed and mandated as part of PPS. M-code provides improved anti-jam and security protection and will allow users easier access to encrypted coding and spectral separation from civil (unencrypted) signals. At that point, PPS will include both the legacy PPS basic signal (the current P(Y) signal) and the new PPS enhanced signal (M-code). Note: GPS M-code is not operationally available, as the user and control segments are still under development.

(1) DoD PNT users may use civilian GPS augmentations for peacetime operations where such use does not jeopardize carrying out military missions. Examples include the U.S. Coast Guard's (USCG) Differential GPS (DGPS), and the Federal Aviation Administration's space-based Wide Area Augmentation System (WAAS) and airport ground-based Local Area Augmentation Systems (LAAS).

(2) It is essential that users understand that civil augmentation systems may not be reliable during conflict, as they do not incorporate the same level of security and survivability as military systems (e.g., the GPS PPS). For examples of some of the DoD systems that should help overcome these security/survivability issues go to Enclosure B, paragraph 2.

f. Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Systems Timing Policy. DoD C4ISR systems that rely on GPS for timing shall use only properly keyed PPS receivers and incorporate the capability to operate without continuous GPS availability or integrity. More detailed information on DoD precise timing systems can be found in Enclosure J.

3. Responsibilities. The responsibilities of DoD organizations for PNT systems are delineated in DoD Directive 4650.05, "Positioning, Navigation, and Timing" and in the DepSecDef's memorandum "Recommendation for the Future Designation of the OSD Principal Staff Assistant (PSA) for Positioning, Navigation, and Timing (PNT) (OSD001790-12) (see Enclosure O, references c and d)." Additional responsibilities are as follows:

a. CJCS is responsible for all operational DoD PNT matters. These functions include:

(1) Developing joint doctrine for use of PNT equipment.

(2) Reviewing Service budgets to ensure appropriate funding of validated PNT and NAVWAR requirements, avoid duplication of effort, and recommend budget alternatives based on operational risk assessments.

(3) Participating as Tri-chair of the DoD NAVWAR Working Group (NAVWAR WG).

FOR OFFICIAL USE ONLY

(4) Coordinating PNT matters affecting NATO, allies, and coalition partners.

(5) Providing direction and inputs for the development of a PNT systems architecture that describes operating concepts, system developments, replacement plans, and alternatives for satisfying validated requirements that are net-centric, standardized, interoperable and compatible.

(6) Participating in PNT committees and working groups, as required.

(7) Preparing, reviewing, and publishing this CJCS MPNTP in coordination with the Department of Defense Chief Information Office (DoD CIO), the Under Secretary of Defense for Acquisition, Technology and Logistics (USD/AT&L), the CCMDs, Military Departments and Defense agencies.

(8) Approving operational concepts and plans that establish PNT security requirements and procedures.

(9) Representing warfighter interests in the DoD SAASM Waiver Process.

(10) Review and screen waiver requests for relief from PNT policy and/or other mandated requirements that include waiver provisions or changes to KPPs or KSAs. This review process is aimed at reducing risk to the operational user only. If approved, a waiver request will then be forwarded to OSD to address policy and acquisition requirements.

(11) Developing and conducting a formal follow up and review process of programs granted OSD SAASM waivers.

(12) In collaboration with OSD, review Foreign Military Sales (FMS) of programs which include GPS SAASM equipment or technology.

NOTE: The CJCS may delegate one or more of the above responsibilities to the Joint Staff, the CCMDs or the Services. Several of those delegations are listed in this instruction.

b. Within their respective commands, combatant commanders perform functions of the same general nature as those of the CJCS, including planning for the operational employment of PNT and NAVWAR systems in war or contingencies. Combatant commanders (CCDRs) may develop PNT requirements in support of contingency plans and CJCS-directed or Joint Staff-coordinated exercises that require not only their own but also other PNT resources. CCDRs are also responsible for reviewing this MPNTP annually,

FOR OFFICIAL USE ONLY

suggesting changes, documenting new JROC-validated requirements, and providing Subject Matter Expertise (SME) to various PNT/NAVWAR-related product teams and working groups. Once approved, the CCMDs and Services will implement this MPNTP.

c. Commander, U.S. Strategic Command (CDR, USSTRATCOM), is the Title 10 authority and has the Unified Command Plan (UCP)- responsibility to plan and conduct space force enhancement operations, which includes space-based positioning, navigation, and timing (PNT) provided by the GPS constellation. Specific responsibilities of CDR, USSTRATCOM include:

(1) Operate GPS in accordance with reference c.

(2) Operate the PPS in accordance with reference e.

(3) Operate the Standard Positioning System (SPS) in accordance with reference f and Enclosure D.

(4) Operate the GPS Operations Center (GPSOC), 24 hours a day (7 days a week), through the Joint Functional Component Command for Space (JFCC SPACE) and the 2nd Space Operations Squadron (2 SOPS).

(5) Provide oversight of the Joint Navigation Warfare Center (JNWC) through JFCC SPACE.

(6) Maintain all GPS and NAVWAR related CONOPS.

(7) Perform key controlling authority responsibilities for all GPS PPS crypto keys issued to U.S. and allied military users, and any other non-military users authorized access to PPS by the Department of Defense. As such, USSTRATCOM is delegated the authority to direct processes and procedures necessary to fulfill these responsibilities, including those that impact technical requirements for future user equipment.

(8) Identify, analyze, and advocate for capabilities and resources needed to accomplish USSTRATCOM's assigned missions related to GPS and NAVWAR. This includes performing as tri-chair (with CJCS and DoD CIO) of the DoD Navigation Warfare Working Group.

d. The Air Force serves as the executive agent to organize, train, and equip, all aspects of the GPS satellite constellation operations.

(1) Air Force Space Command's (AFSPC) Space and Missile Systems Center (SMC) at Los Angeles Air Force Base (AFB), CA, is the center of technical excellence for researching, developing and acquiring military space systems.

FOR OFFICIAL USE ONLY

(2) The GPS Directorate (SMC/GP) is a joint service organization directed by the Air Force and managed at SMC. The SMC/GP is the DoD acquisition office for developing and producing GPS satellites, ground systems, common military user equipment, GPS security devices/components, standards and interface control documents.

(3) 2 SOPS, 50th Space Wing, and AFSPC operate and control the GPS constellation.

(4) HQ AFSPC, through the Operations and Maintenance Program Element Monitor, will ensure proper funding POM and advocate funding for GPS operations across the FYDP.

e. NGA is responsible for Geospatial Information and Services (GI&S) support to DoD navigation systems. The support includes the production, maintenance and distribution of charts, digital terrain elevation data (DTED), digital feature analysis data, digital hydrographic chart data, approved digital aeronautical information, point-positioning data bases, geodetic surveys, the World Geodetic System 1984 (WGS 84), Deflection of the Vertical (DoV), World Magnetic Models (WMM), Digital Vertical Obstruction File (DVOF), and associated tables that are compatible with and meet the accuracy objectives approved by the CJCS. GI&S support also includes geodetic positioning of transmitters for electronic systems and tracking stations for satellite systems, maintenance of GPS fixed site operations, digital gravity data supporting high accuracy INS, and generation and distribution of GPS precise ephemeris. NGA serves as the primary point of contact with the civil community on matters relating to geodetic uses of DoD navigation systems and provides calibration and accuracy support for certain land based, airborne, marine, and space based navigation systems.

f. The National Security Agency (NSA) is responsible for the development and maintenance of GPS cryptography. The NSA, through Information Assurance (IA), assists in design of devices and techniques used to protect PNT systems information from unauthorized access. NSA is responsible for educating all other DoD agencies on actual and suspected PNT cryptographic vulnerabilities. NSA is responsible for the development of all key management architectures for GPS and for developing or certifying all GPS crypto key-loading devices. NSA is the certifying agency for the security of Selective Availability/Anti-Spoofing Module (SAASM) devices, the Block III M-Code Generator on the space vehicle, and the Ground Control Segment Application Uplink Encryptor. The GPS Directorate is the certifying agency for M-code capable Military GPS User Equipment (MGUE). This includes validating information assurance certification of PPS UE for unattended/unmanned operations.

FOR OFFICIAL USE ONLY

g. The Secretary of the Navy, through U.S. Naval Observatory (USNO), is responsible for:

(1) Deriving and maintaining standards for both Precise Time and Time Interval (PTTI) and ensuring uniformity in PTTI operations. UTC (USNO), as determined by the Master Clock at USNO, is the Department of Defense time standard. The output of the Master Clock is the reference for GPS.

(2) Establishing and maintaining the astronomical reference frame(s) for celestial navigation, the background astronomical reference frame (used for detecting/tracking of space-borne objects), and the orientation of space systems. USNO produces astrometric (star) catalogs, Earth orientation parameters, almanacs, software products, and data services to meet DoD operational needs for navigation and referencing. Celestial Reference Frame (CRF) USNO (CRF-USNO), as determined by the USNO astrometric catalog(s), is the DoD orientation and astrometric reference frame standard.

h. The National Space-Based Positioning, Navigation, and Timing (PNT) Executive Committee (EXCOM) is the senior-level USG body established by the President's Policy for Space-Based PNT (see Enclosure O, reference g) to advise and coordinate among member Departments and Agencies responsible for the strategic decisions regarding policies, architectures, requirements, and resource allocation for maintaining and improving U.S. space-based PNT infrastructure. The National PNT EXCOM is co-chaired by the Deputy Secretaries of the Department of Defense and the Department of Transportation (DOT). Membership of the National EXCOM includes representatives, at the equivalent level of the co-chairs, from the Departments of State, Commerce, and Homeland Security, the Joint Chiefs of Staff, and the National Aeronautics and Space Administration. The EXCOM advises and makes recommendations to its member Departments and Agencies that ensure services provided by U.S. space-based PNT infrastructure, including GPS and GPS augmentations, are made available and consistent with the U.S. Space-Based PNT Policy (see Enclosure O, reference g) in support of national security, homeland security, foreign policy, economic issues, public safety, and scientific interests.

i. The National PNT Executive Steering Group (ESG) is the next-level below the National PNT EXCOM. It is co-chaired by DoD CIO and the Assistant Secretary of Transportation for Policy. The ESG reviews all briefings and issues (for information, coordination or decision) before presentation to the EXCOM.

j. A National Coordination Office (NCO) for Space-Based PNT is responsible for the mission, objectives, and goals of the EXCOM and ESG. The NCO is led by a full-time Director who functionally reports to the EXCOM and ESG co-

FOR OFFICIAL USE ONLY

chairs and performs designated responsibilities and functions on behalf of the EXCOM.

k. The DoD PNT EXCOM is chaired by DoD CIO, and reviews and coordinates military/interagency PNT issues. These issues could pertain to the Department of Defense, its military allies, or upcoming topics at the National PNT ESG or EXCOM. The DoD PNT EXCOM advises and makes recommendations to the National PNT EXCOM, ensuring minimum interference and intrusion of the electromagnetic spectrum (EMS) that could affect GPS PNT operations. See Enclosure O, reference h for more details.

FOR OFFICIAL USE ONLY

ENCLOSURE B

PNT REQUIREMENTS

1. General Requirements. It is DoD policy to develop, procure, sustain and modernize PNT systems to meet the full spectrum of military operations. The PNT Joint Capabilities Document (JCD) (see Enclosure O, reference i) and PNT Assurance Initial Capabilities Document (ICD) details elements necessary to meet operational requirements. Requirements for PNT systems and systems of systems can include the following, depending on the user's needs:

a. Provide worldwide coverage.

b. Be user-passive and include active exchange of information when closed loop Monitoring and Control of the end-user device is required.

c. Enable U.S. denial/degradation of adversary use while not impacting friendly military operations or unduly disrupting civil users.

d. Be able to support an unlimited number of users.

e. Be resistant to countermeasures. Systems should be as survivable and durable as the forces and weapon systems they support including resistance to hostile attack, inadvertent/unintentional electromagnetic interference, electromagnetic pulse (EMP), and natural disturbances.

f. Possess system integrity.

g. Remain reliable through all levels of conflict.

h. Provide real-time response.

i. Maintain interoperability among DoD Services and Agencies, allied and/or coalition partners and non-DoD agencies that interface with the CCMDs.

j. Remain free from spectrum, bandwidth, and frequency allocation problems.

k. Provide common grid or map datum reference for all users.

l. Provide common time reference for all users.

FOR OFFICIAL USE ONLY

m. Maintain accuracy and availability that is not excessively degraded by changes in location, altitude, high-"G" or other abrupt maneuvers, weather, complex terrain changes, or by time of year or day.

n. Be maintainable and sustainable.

o. Be self-contained.

p. Provide four-dimensional information (i.e. x, y, z, and time).

q. Be certifiable for applications involving civil land, maritime, and airspace operations.

r. Indicate degradation of service due to interference (i.e. jamming, multi-path, weather and terrain effects, spoofing) and provide this information to electronic support (ES) efforts to detect, identify, and resolve interference issues.

2. Operational Survivability Requirements. PNT User Equipment should be designed to be as survivable and robust as the forces, communication, infrastructure, and weapon systems they are designed to support, or in which they are integrated. Terrestrial-based systems, such as: Tactical Air Navigation (TACAN), Microwave Landing System (MLS), Instrument Landing System (ILS), etc., should employ physical security measures that reduce vulnerability to sabotage or terrorist attack. Rapid reconstitution plans, including plans for replacement transmitters, use of rugged construction techniques, conventional and nuclear hardening, and armed guards should be considered. Physical security measures must be in place to minimize the impact of attempts to destroy or incapacitate space-based PNT ground control segments. Transmission and reception techniques to minimize jamming and other interference must be employed. Additionally, methods need to be employed and CONOPs developed to minimize hostile exploitation of PNT systems and to deny use of such systems, when directed, to military adversaries or other unfriendly combatants (see Navigation Warfare, Enclosure E).

3. Aviation Requirements

a. Aircraft must be equipped with instruments and navigation equipment appropriate to the routes to be flown. The FAA issues Technical Standard Orders that prescribe minimum performance standards for navigation equipment used by the civil aviation community in the National Airspace System (NAS). The International Civil Aviation Organization (ICAO) issues standards and recommended practices (SARPS) for international civil aviation. The DoD self-certifies PPS for use in the NAS and international airspace. The DoD operates a standards program known as Military Standards Orders

FOR OFFICIAL USE ONLY

(MSOs) that is similar to the civilian FAA Technical Standards Orders (TSOs) program. MSO C145 refers to airborne navigation sensors using GPS PPS for area navigation (RNAV). These military standards must conform to civil airspace required navigation performance requirements, prevent violation of civil air traffic clearances, and ensure safe separation of military and civil air traffic. While meeting the ICAO SARPS is essential, military combat and combat support aircraft must have PNT capabilities designed to operate in a combat or stressed environment, including a GPS-denied environment. The DoD will consider equivalent civil performance standards in determining its aviation navigation needs and certify its PNT equipment for military aviation use.

b. The Department of Defense works with military establishments of its international allies as well as the ICAO to seek approval for use of PPS in foreign airspace. It will provide an enhanced capability to span the operational environment for military aviation from flight in civil airspace in peacetime to combat operations worldwide.

c. The Department of Defense does not establish requirements for the use of civil GPS signals nor for the use of other GNSS signals. It should be noted that legacy and current military GPS receivers use L1 C/A code and future receivers may use L1 C/A, L1C, L5 and/or L2C for specific applications. Consequently, in no case should a decision be made to alter the civil, as well as military, signal structure without consulting the CJCS. In no case shall a U.S. military system (or system supporting U.S. military operations) rely solely on civil or foreign systems (without appropriate waiver), but may use them to augment PPS performance when appropriate measures are taken to provide information assurance for PNT. L5 UE may be included in the future on a limited number of military airframes on a case-by-case basis (with appropriate waivers in place). These airframes could include the CRAF if commercial operators elect to use L5; National Guard and Reserve Component aircraft if there is a demonstrated benefit from L5 at civil airports where these aircraft operate; and civil-derivative military aircraft that may include L5 as normal equipment.

d. Joint Precision Approach and Landing System (JPALS), Capability Development Document (CDD) dated 6 April 2007, Increment 1 and 2, is an all-weather, all mission, all-user landing system based on local area differential GPS PPS. JPALS works with GPS to provide accurate and reliable landing guidance for fixed and rotary wing aircraft during all weather conditions. It features high GPS anti-jam protection to assure mission continuity in a hostile environment. JPALS equipment supports fixed-base, tactical, and shipboard applications. It is compatible with civil and military GPS signals. The JPALS system is being developed to provide a secure, jam-resistant all weather

FOR OFFICIAL USE ONLY

Category I/II/III aircraft landing system that will be fully interoperable with planned civil systems utilizing the same technology.

FOR OFFICIAL USE ONLY

ENCLOSURE C

PNT SYSTEM ARCHITECTURE

1. General. Currently no single PNT system exists to support all DoD PNT requirements as outlined in Enclosure B. Therefore, the DoD PNT architecture summarized in this enclosure consists of a mix of PNT systems.

2. Architecture. The DoD PNT architecture consists of systems that are used in combat, combat support, and combat service support operations and systems that support worldwide non-combat operations. The challenge for the Department of Defense is to minimize the costs to equip platforms to operate in both environments while eliminating the necessity to maintain duplicative systems.

a. Systems utilizing PNT for combat, combat support, and combat service support. Below are general descriptions of combat, combat support and combat service support categories.

(1) Combat: Those systems/elements that directly engage the enemy (e.g., fighter/bomber/attack aircraft, guided-munitions, infantry, armor, front-line artillery, special ops/forces, Unmanned Aircraft Systems (UAS), etc.).

(2) Combat Support: Those elements that provide support and other operational assistance to combat elements (e.g., C4I, ISR, military police, combat search and rescue, combat engineers, etc.).

(3) Combat Service Support: Those elements whose primary missions are to provide service support to combat forces and which are a part, or prepared to become a part, of a theater, command, or task force formed for combat operations (e.g., logistics, maintenance, ordnance, supply, transportation, health services, etc.).

b. Non-combat Operations. The 2010 Federal Radionavigation Plan (FRP) contains descriptions of federally provided PNT systems that are available for non-combat applications for DoD platforms. DoD users are reminded of the policy as stated in Enclosure A of this document on the use of civil PNT systems for combat and non-combat operations.

3. Current PNT Systems Architectures. The DoD PNT architecture consists of a mix of PNT systems; however, GPS is the primary radionavigation system source of PNT information for the Department of Defense.

4. Future PNT Systems Architectures. Determination of what PNT systems are to be maintained to fulfill DoD requirements is a function of the mission

FOR OFFICIAL USE ONLY

criticality being served by a specific PNT system, the redundancy requirements necessary to conduct a DoD mission, and costs (operations and maintenance). The DoD PNT Science and Technology (S&T) working group tracks the development of new PNT systems and their applicability to future combat, combat support, and combat service support operations. Enclosure G of this document lists other PNT systems being studied or developed to complement GPS.

a. The GPS III Capabilities Development Document (CDD) (see Enclosure O, reference j), approved in 2009 by the JROC (see Enclosure O, reference k), provides capabilities development guidance.

b. An effort is currently underway to certify PPS receivers for operations in controlled airspace. The Deputy Chief of Staff, Air, Space & Information Operations, Plans & Requirements (AF/A3/A5) has the DoD lead in evaluating the use of GPS PPS in controlled airspace. The Army and Air Force GATM architectures represent the effort to ensure appropriate aircraft comply with FAA and/or ICAO communications, navigation, surveillance, and air traffic management requirements. The Navy has a similar program to ensure compliance with FAA and/or ICAO requirements and refers to it as Communication Navigation Surveillance/Air Traffic Management (CNS/ATM).

FOR OFFICIAL USE ONLY

ENCLOSURE D

GPS: OPERATIONS, SECURITY POLICY, AND RESPONSIBILITIES

1. Policy. The Military Services, Joint Staff, CCMDs, and Defense agencies will comply with established policies, specifically:

a. National Security Presidential Directive Policy, Number 39, U.S. Policy for Space-Based Positioning, Navigation, and Timing (NSPD-39), 8 December 2004

b. DoD Directive 4650.05, Positioning, Navigation and Timing, 19 February 2008

c. DoD Global Positioning System Security Policy, April 2006

d. Unified Command Plan (Change 1, 2011)

e. National Space Policy, 28 June 2010

2. Summary

a. The Department of Defense operates the GPS PPS to provide a military advantage for the United States and its allies. PPS COMSEC release is controlled through an approval process described in CJCSI 6510.06 "Communications Security Releases to Foreign Nations" (see Enclosure O, reference l). PPS UE release is controlled through a process described in DoD GPS Security Policy (see Enclosure O, reference e). This process is initiated by CCMDs when required for interoperability with allies. While GPS SPS is available for peaceful civil, commercial, and scientific use on a continuous, worldwide basis, free of direct user fees, it is anticipated that adversaries may attempt to use GPS SPS for hostile purposes.

b. In accordance with National Space-Based PNT Policy (Enclosure O, reference g) and Enclosure E of this instruction, the Department of Defense intends to prevent adversary use of GPS and any space-based PNT services during hostilities, without unduly interfering with the peaceful use of GPS outside an area of operations. DoD, allied, and friendly foreign military GPS users will use the PPS to ensure enhanced availability and exclusivity of GPS. The following paragraphs detail the overarching GPS operational, security, and NAVWAR related policies and responsibilities.

3. SPS and PPS Policy

a. Positioning Policy.

FOR OFFICIAL USE ONLY

(1) Use of commercial GPS receivers must not affect the ability of an individual, unit or platform to employ keyed PPS-capable receivers to conduct military operations. GPS enabled military operations, such as weapons delivery coordination, target location, fire support, in-flight refueling, close air support, ISR, extraction, rendezvous, etc., will only be performed in training, exercise, or combat, with properly keyed PPS-capable GPS user equipment. This includes the need to use keyed PPS-capable UE during training and exercises involving the operational use of PPS UE. At no time will such critical operations be performed with SPS GPS receivers

(2) Waivers for use of SPS in lieu of PPS. All acquisitions that incorporate GPS to perform or enable military operations must acquire GPS receivers (SAASM or MGUE) able to operate in the keyed PPS mode. Requests for waivers to use SPS vice PPS in combat support and combat service support acquisition programs shall be submitted to OSD via the Joint Staff/J-6 (IAW Enclosures L and M) for review of possible undue operational impact. If unintended negative impacts are satisfactorily addressed and deemed operationally essential, the Joint Staff/J-6 will route requests to OSD for acquisition policy waiver consideration. All of the following criteria must be met:

(a) The requesting COCOM, service, or agency sponsors the waiver request (Enclosure K and M) through the Joint Staff FCB and JCB process (Enclosure K). The requesting Service states that use of SPS results in limited or no reduction in mission capability of the host platform or system when operating in a jammed or otherwise electronically challenged environment. Additionally, the COCOM, service, or agency must show that no undue operational impact is imparted to users of the system. Any reduction in capability must be described in terms of all affected Key Performance Parameters (KPPs) and Key System Attributes (KSAs). If a KPP or non-delegated KSA is negatively affected by the use of SPS, the waiver request must be processed via CJCSI 3170.01H process for JCIDS change request. The waiver request must include a statement from the requirements authority acknowledging and accepting the associated effects and risks. Waivers are granted on a temporary basis.

(b) The requesting Sponsor provides an approved plan for incorporating the proper PPS GPS (SAASM or MGUE) receiver into the platform, system or device (approved by the designated milestone decision authority).

(c) The requesting Sponsor provides a program, approved by the service's operations office, to plan and train for operational performance of the receiver purchased and employed under the waiver. This training must

FOR OFFICIAL USE ONLY

highlight the vulnerabilities of SPS use and the means to detect and mitigate GPS interference and jamming.

(d) A signed memorandum from the Service Acquisition Executive addressing the risks and describing the mitigations to the issues in paragraphs 1), 2) and 3) above.

(e) Due to dwindling numbers of PPS-SM devices, waivers requesting the use of older Legacy PPS for new GPS enabled systems will only be considered as part of the formal Legacy GPS Waiver Working Group process. If the GPS waiver working group is not established, requests shall be submitted to Joint Staff J-6. Per DoD GPS Security Policy (Enclosure O, reference e), commercial (SPS-only) receivers may be authorized for Operations and Maintenance (O&M) purchase and use for limited non-critical applications to enhance individual situational awareness and logistics material tracking without the requirement for a DoD waiver, provided the commander of the purchasing unit publishes (or implements higher headquarters) procedures which ensure all of the following conditions are met:

(1) The services and Combatant Commands (CCMDs) plan and train for operational performance of receivers purchased under this exemption to be no better than the performance capabilities published in the "Global Positioning Systems Standard Positioning Service Performance Standard" (Enclosure O, reference f).

(2) USSTRATCOM, National Security Space Institute (NSSI) and Service components will be responsible for ensuring individual users and units are educated on the inherent weaknesses of the SPS signal, especially the lack of encryption resulting in its increased vulnerability to jamming and significant vulnerability to spoofing. Appropriate tactics, techniques, and procedures (TTPs) will be developed to provide operational training and exposure to the impact of such threats on the capabilities and use of commercial (SPS) GPS receivers.

(3) SPS waiver sponsors will be responsible for ensuring Allied, DoD, and associated support personnel utilizing commercial GPS (SPS) are educated and trained that such use on the battlefield is merely an augmentation to PPS and is available only as a convenience for situational awareness. Do not plan, train, exercise, or operate in a manner that considers use of SPS receivers in determining the need for, or the execution of, NAVWAR denial of the SPS signal within an area of operations.

NOTE: Title 10, U.S.C., section 2281 note (Pub L. 111-383, Sec 913) states that all DoD GPS user equipment purchases made after 2017 must be capable of receiving M-Code. Civilian vehicles are excluded. The Secretary of Defense

FOR OFFICIAL USE ONLY

may grant waivers to this law if the Secretary determines that suitable UE capable of receiving the M-Code is not available or does not require that user equipment to be capable of receiving the military code from GPS.

(f) Exceptions to the Waiver Process. In some cases, Services and DoD Agencies are required to acquire platforms, systems, and devices that are intended for use in non-combat, non-critical operations. Per reference e, SPS receivers are authorized for non-critical applications to enhance situational awareness and logistics tracking without the requirement of an OSD waiver. In these cases, the program manager or commander of the purchasing unit must provide OSD and JS/J-6 with a memorandum affirming that the intended platform, system or device will only be used in non-combat or non-critical operations, and that use of GPS in the acquisition is intended for situational awareness or logistics tracking only.

b. Timing Policy

(1) The DoD reference standard for PTTI is established by the Department of the Navy's USNO. The Superintendent, USNO is directed by reference h to act as the DoD PTTI manager. UTC (USNO) is Coordinated Universal Time as provided by USNO. Each DoD platform/system that uses precise time or precise frequency shall use UTC (USNO) as its reference standard (see Enclosure O, reference m). In support of the Defense Information Infrastructure, DoD PTTI users (particularly those who require UTC (USNO) as delivered by GPS as their primary timing source) will procure and use GPS PPS receivers. USNO may provide equally accurate direct services to select activities as the situation arises.

(2) PTTI is critical for many DoD systems. Although not always readily apparent to the users of the system, timing information is often obtained by using GPS. It is important that the GPS delivery of UTC (USNO) time be assured by using keyed PPS UE. If DoD users are relying upon SPS timing sources, then any disruptions of SPS signals can also disrupt the timing information. The acquisition and waiver process described above apply to all DoD systems utilizing GPS for PTTI. Since intentional NAVWAR actions or unintentional electromagnetic (EM) transmissions may disrupt SPS signals throughout an area of operations, DoD users that rely on SPS delivered timing sources will likely be negatively impacted by the denial efforts. This denial or disruption of the GPS "navigation" signals may also impact warfighter systems (such as networks) which rely on PTTI.

c. Celestial Reference Frame (CRF) Policy

(1) The DoD standard for the celestial reference frame and Earth orientation parameters is the CRF-USNO and Earth Orientation Parameters

FOR OFFICIAL USE ONLY

(EOP) as established by the Department of the Navy at the USNO. All DoD systems that use all or part of the CRF or EOP shall use these reference standards. There are exceptions to this policy.

(2) Astrometry provides the extremely precise observational and astrophysical techniques together with the observational data and analysis required to produce the celestial reference frame, and provides the basis for autonomous navigation, very precise ISR orientation, orbit determination for Space Situational Awareness (SSA) applications, and high-accuracy targeting. Astrometry is the branch of astronomy that relates to precise measurements and explanations of the positions, distances, and movements of stars and other celestial objects.

(3) Earth Orientation is the determination and prediction of the time-varying alignment of the Earth's terrestrial reference frame with respect to the inertial or celestial reference frame. Earth orientation includes modeling the motions of the Earth and measuring the changes caused by geophysical processes. The Earth Orientation Parameters (EOP) are mathematical relationships between the terrestrial reference frame (WGS 84) and the "inertial" or celestial reference frame and is critical for high-accuracy positioning and targeting. This relationship is defined by the coordinates of the Earth's pole (polar motion), the rotation angle about the pole (Universal Time or UT1), precession, and nutation/irregularity.

d. DoD Differential Policy. Differential GPS (DGPS) techniques are used to increase the accuracy and/or integrity of the SPS and PPS signals. In general, DGPS methods involve the transmission of error correction information to GPS user equipment via a communications link. The error correction information enables UE to compute position or timing solutions to a higher level of accuracy than can be achieved solely through the use of the basic SPS or PPS services. There are significant civil, as well as military, uses of DGPS.

(1) The DoD intends to operate using the PPS signal in space as the primary source of PNT data for military operations. However, to satisfy high-precision PNT requirements of military platforms, the DoD is developing methods to raise the accuracy directly available from PPS to levels previously obtainable only through the use of DGPS techniques. However, should a DoD user need DGPS for combat operations, the differential systems employed must use PPS, and the differential corrections must be encrypted for transmission and processing.

(2) Augmentation of modernized PPS includes integration of external information in the navigation calculation process. In addition to INS and differential systems, this may include the use of civil GPS signals, integration with non-RF sources, and signals from other GNSS when appropriate measures

FOR OFFICIAL USE ONLY

are taken to provide information assurance for PNT, and PPS is used as the trusted RF source. To support this, NGA is developing a GNSS performance monitoring capability to provide DoD users a near real time measure of the performance of foreign GNSS systems, with Initial Operational Capability (IOC) planned for FY 2015.

(3) Use of SPS DGPS by DoD users requires an OSD waiver unless the basic SPS use is waived or exempted under other sections of this instruction.

(4) The DoD plans to deny SPS DGPS services in local combat theaters or other areas in accordance with national security interests.

4. Security Architecture Requirements/Responsibilities

a. Selective Availability/Anti Spoofing Module (SAASM) and Military GPS User Equipment (MGUE) Policy. DoD GPS Security Policy requires the use of SAASM in all newly fielded systems, as well as systems going through major modifications or upgrades (see para 4.a.(2) below.) The SAASM architecture is currently replacing the existing legacy PPS Security Module (PPS-SM) Auxiliary Output Chip (AOC) architecture and will, in turn, be replaced over time by M-Code capable Military GPS User Equipment (MGUE). The length of time necessary to transition to MGUE will require that PPS users operate with a mix of legacy, SAASM and M-Code capable UE. More details on SAASM Operations can be found in the SAASM Concept of Operations (CONOPs) (see Enclosure O, reference n). The GPS Directorate and NSA are presently developing an improved GPS security architecture for use by MGUE. To ensure backwards compatibility, the MGUE will acquire and track the civil-code, Y-code and M-code, as well as use new cryptographic logic and users' keys. The following policies apply:

(1) Until MGUE is available for acquisition, all newly fielded DoD systems using GPS shall use SAASM PPS devices. When MGUE is available, all newly fielded DoD systems using GPS shall acquire MGUE. In any case, IAW public law 111-383 section 913, all DoD GPS user equipment purchases made after 2017 must be capable of receiving M-Code.. The SMC/GP and the Services will no longer support the procurement of legacy PPS-SM components unless approved by OSD. DoD agencies that may require continued use of legacy GPS PPS-SM devices for acquisition programs must pursue a waiver as described in paragraph D-3 and Enclosure K. The new GPS Security Architecture developed by the SMC/GP and NSA for MGUE is approved for use on SAASM devices. The SMC/GP will be the security certification authority for SAASM and MGUE.

(2) Existing operational systems with legacy PPS receivers (procured prior to 1 October 2006) will not be required to retrofit to SAASM to achieve

FOR OFFICIAL USE ONLY

compliance, and SAASM equipment procured prior to the availability of MGUE will not be required to retrofit to SAASM to achieve compliance. Existing operational systems with legacy PPS receivers will not be required to retrofit to SAASM to achieve compliance. However, whenever an operational system plans to upgrade from a non-GPS equipped subsystem or an upgrade or modification to its GPS-equipped subsystem, it shall incorporate SAASM or MGUE, unless it will be removed from service within 5 years. Routine operational maintenance and warranty repair of fielded systems are excluded. However, legacy equipment needed for Service Life Extension Programs (SLEP), or a life extension that could be interpreted as SLEP, requires an approved OSD waiver.

(3) The FY2011 NDAA, public law 111-383 sec 913 states that all DoD GPS user equipment purchases made after 2017 must be capable of receiving M-Code. Once low rate initial production of certified MGUE begins, the Joint Staff reserves the right to mandate that some platforms retrofit from legacy PPS UE to MGUE to support NAVWAR operations.

(4) Systems not complying with paragraphs (1) and (2) above must obtain a waiver IAW Enclosures D and L. After FY2017, systems not complying with paragraph (3) above must obtain a waiver from the SECDEF. Waiver requests must document why M-code capable UE are not available or why M-code capable UE are not required and the forecast compliance date (month/year) for use of SAASM or MGUE.

(5) If waivers are still required past a previously approved compliance date, they must be resubmitted for extension.

b. GPS Anti-Tamper Security. GPS security devices installed in PNT systems for operational use or export shall incorporate approved Anti-Tamper (AT) mechanisms:

(1) Legacy PPS-SM: NSA determines anti-tamper requirements.

(2) SAASM: NSA determines anti-tamper requirements.

(3) MGUE: GPS Directorate determines anti-tamper requirements based on an AT level in coordination with the DoD AT Executive Agent (EA).

NOTE: DoD or Service offices involved in initiating or approving FMS or DCS shall not do so for any PPS-equipped systems that contradict this instruction.

c. Users requiring (routine and contingency) SAASM reprogramming in the field shall provide an interface adapter (and path) capable of transferring data from the mobile Key Data Processor (KDP) Loading and Initialization Facility

FOR OFFICIAL USE ONLY

(KLIF) to the KDP within the SAASM. The adapter will meet the Interface Specifications of IS-160-GPS. KLIF personnel will notify NSA and the SMC/GP prior to any non-standard KDP reprogramming.

d. Red Key to Black Key Transition. A security benefit of SAASM and MGUE is the ability to significantly reduce the distribution of red (classified) keys. The SAASM architecture is designed to enable the full acceptance and implementation of black (unclassified) keys, and thus increase the security of GPS PPS. This transition will reduce, to the absolute minimum, the distribution of red GPS key consistent with operational needs.

e. The appropriate key for operational mission requirements shall be available as required throughout the transition from legacy to SAASM and ultimately to the modernized military code (M-code in MGUE) security architectures. Red keys will continue to be issued by NSA and USSTRATCOM to programs whose GPS UE will not accept black keys and for SAASM-based systems that require red key for interoperability. Units with SAASM-based systems that require red key for interoperability will submit waiver requests to USSTRATCOM who will verify the validity of each program's red key request in these cases.

f. At a minimum, SAASM or MGUE must be able to perform the following operational functions:

(1) Process multiple unique data sets across multiple satellite vehicles:

(a) SAASM OTAD/OTAR- Process black keys and accept over-the-air key distribution that matches current primary cryptonet and data from each unique broadcast from all satellites in view. NOTE: Multiple concurrent OTAD/OTAR broadcasts of allied keys will take place in near future as GPS capabilities evolve. Receivers unable to process data from each unique broadcast from all satellites in view will need to rely on traditional key delivery methods or, if mission needs require, modify receiver design to obtain correct key from the multiple concurrent OTAD/OTAR broadcasts.

(b) MGUE OTAD/OTAR- Process, accept, store, and transfer all received unique black key data sets regardless of cryptonet.

(2) SAASM and MGUE- Perform signal authentication.

(3) SAASM and MGUE- Perform contingency recovery.

(4) SAASM and MGUE- Provide physical security of the Security Function Module (SAASM multi-chip module or MGUE) through the use of approved anti-tamper (AT) mechanisms or technologies.

FOR OFFICIAL USE ONLY

(5) SAASM and MGUE- Direct Signal Acquisition: The ability to directly acquire and track GPS PPS signals (i.e., Y-code or M-code) will become essential to operations in stressed environments. Military GPS users now have the capability to directly acquire Y-code signal through appropriately designed SAASM devices. The direct acquisition of the M-code signal is being developed in the MGUE design. Programs that incorporate SAASM into their platforms or systems should include direct signal acquisition capability whenever feasible, and must ensure vendors are aware of the specific timing and correlation requirements which enable direct signal acquisition.

g. Validation of Red and Black Keys. USSTRATCOM will process and approve the release or transfer of GPS keying material, for the use by the US or allied user, as prescribed in their instruction – "Cryptographic Key Ordering Instructions for Precise Positioning Service Users" (Enclosure O, reference o). GPS keys cannot be issued to foreign allies until the user has completed the CJCSI 6510.06 process (see Enclosure O, reference l) and appears on the DoD approved PPS user list contained in the "GPS Security Policy Interim International Supplement," 4 April 2006.

(1) Military Legacy and SAASM Users. Joint Staff/J-6 will only validate new U.S. and foreign military user red weekly key requests. Joint Staff/J-6 has delegated validation of all other military key requests to USSTRATCOM, to include U.S. and foreign requests for: red yearly, or Group Unique Variable (GUV); black yearly, or BGUV; and black monthly. Allied and coalition PPS users already receiving the GUV or red weekly key will automatically be eligible for black monthly key. For red weekly requests from U.S. Military users, USSTRATCOM key controlling authority is granted initial validation authority to meet the end user's operational needs. Coordination and final validation with Joint Staff is still required. USSTRATCOM will send semi-annual updates of this list to Joint Staff/J-6 and NSA for review.

(2) MGUE Users. The validation process for MGUE Black keys has not yet been defined, but will likely be similar to the SAASM black key validation process described above.

(3) Once validated for receipt of GPS key, PPS users should follow USSTRATCOM "Cryptographic Key Ordering Instructions for Precise Positioning" (see Enclosure O, reference o).

h. Key supersession. When circumstances dictate the need for emergency supersession, USSTRATCOM shall expeditiously execute supersession in accordance with approved concepts of operations.

FOR OFFICIAL USE ONLY

i. Cryptography. NSA and the SMC/GP have developed the SAASM and M-Code core cryptography and their associated keys. For SAASM, the black keys within one cryptographic network (CNET) will not be interchangeable with the black keys of any other CNET. Each SAASM (and eventually each MGUE) will be programmed with one Primary CNET and several Alternate CNETs. An Alternate CNET can become the Primary CNET in the UE by uploading the appropriate black key update parameters. Joint Staff/J-6, after consulting with the Air Force, NSA and USSTRATCOM, has specified the number and structure of CNETs in the SAASM CNET Architecture Transition Plan (see Enclosure O, reference p). The M-Code key distribution architecture is similar in that the keys are non-interchangeable and that multiple user groups may be provided a common key for coalition operational use.

5. Security Architecture Responsibilities

a. DoD CIO will:

(1) Provide overarching SAASM and MGUE procurement policy and implementation instructions to GPS developers, acquirers, users and program managers of platforms and systems that implement SAASM or MGUE.

(2) Validate all GPS key requests from U.S. and foreign civil PPS users.

b. The Joint Staff will:

(1) Provide overarching SAASM or MGUE operational implementation policy to U.S. military users of SAASM UE and MGUE.

(2) Review, validate, and forward SPS and SAASM waiver recommendations to OSD.

(3) Review and approve justified KLIF mobilization and priority processing requests.

(4) Coordinate with USSTRATCOM and NSA on the operational implementation and management of emergency key supersession.

(5) After consultation with NSA, USSTRATCOM, and the Air Force, determine the number and structure of black key crypto nets, and publish updates to the SAASM CNET Architecture Transition Plans.

c. NSA will:

(1) Perform Information Assurance (IA) risk assessments and provide IA recommended solutions and requirements.

FOR OFFICIAL USE ONLY

(2) Design, develop, and distribute the GPS black keys and key-related products, including those that support over-the-air-distribution (OTAD) of Black key and any over-the-air-rekeying (OTAR) done out-of-cycle.

(3) In coordination with USSTRATCOM, develop and maintain a GPS Key Management Plan.

(4) Implement the Key Management Infrastructure (KMI) to expedite the delivery of black keys and key products to GPS PPS users.

(5) Support appropriate organizations in the development of IA policies to enhance GPS security.

(6) Coordinate on SMC/GP security approvals for GPS UE designed for unattended/unmanned operations.

(7) Coordinate on PPS devices included in FMS and DCS.

d. The SMC/GP will:

(1) Develop the functional and security requirements for SAASM and MGUE.

(2) Approve SAASM and MGUE functional, operational and security requirements after consideration of NSA's IA risk assessment and user concurrence.

(a) SAASM functional and security requirements include: OTAR; signal authentication and contingency recovery; GPS black key CNETs; KLIF; and positive control of GPS security devices throughout development, integration, and fielding.

(b) MGUE functional and security requirements will include similar capabilities, including OTAR, contingency options, and an initialization function, but may be implemented differently.

(3) Write specification for GPS keys.

(4) Support appropriate organizations in the development of IA Policies.

(5) Recommend the number and structure of CNETs and coordinate with USSTRATCOM and NSA to implement the Joint Staff approved SAASM CNET Architecture Transition Plan (see Enclosure O, reference p).

FOR OFFICIAL USE ONLY

(6) Establish and manage the SAASM KDP developer to design, develop, maintain and plan improvements for the SAASM KDP.

(7) Establish and manage the MGUE developer to design, develop, maintain, and plan improvements for MGUE.

(8) Establish and manage the SAASM KLIF.

(9) Develop and execute a GPS UE security approval process to ensure GPS UE developer compliance with SMC/GP security requirements.

(10) Develop and maintain a single capability for a GPS signal simulator that implements all SAASM functions, including OTAR and contingency recovery features.

(11) Act upon requests for the development and use of a GPS simulator, or equivalent, capable of performing the SAASM OTAR or CR security feature after coordination with the Joint Staff/J-6 and NSA.

(12) Develop and maintain a set of software requirements and test vectors for GPS signal simulators that simulate the SAASM security and functional requirements.

(13) In collaboration with NSA, review, evaluate, and approve appropriate requests for the development and use of a GPS simulator, or equivalent, capable of performing SAASM's OTAR or CR security feature.

(a) SAASM simulators, or equivalent, capable of performing SAASM's OTAR or CR security feature, shall be for U.S. government use only.

(b) The SAASM Black Key Algorithm (BKA) shall <u>not</u> be implemented in any GPS signal simulator.

(c) Ensure organizations, agencies and entities intending to develop or use SAASM simulators, or equivalent, will submit a request to the SMC/GP for approval. More detailed simulator policy is found in reference e.

(14) Develop and maintain M-Code simulators.

(15) In collaboration with NSA, review, evaluate and approve appropriate requests for the development and use of M-Code capable GPS simulators, or equivalent.

(16) Validate contractor requests for GPS SAASM black key material and forwards validated requests to USSTRATCOM.

FOR OFFICIAL USE ONLY

(17) Establish and manage the MGUE software loading process. The design of the MGUE and its software loading capability are still in development.

(18) Review and approve the designs of U.S.-developed GPS PPS user equipment to ensure compliance with GPS security requirements. Publish security requirements and guidelines for the security review and approval of GPS PPS user equipment, including PPS HAE, PPS signal transmitters, and PPS security devices. SMC/GP security approval of U.S.-manufactured PPS hardware and software is required prior to their operational use by authorized U.S. PPS users and prior to their export to authorized foreign countries. The SMC/GP will also develop and release documents to control the development and the use of other GPS signal transmitters, GPS PPS test equipment, and mission planning systems.

(19) The SMC/GP will develop, implement and maintain GPS performance evaluation and security certification programs for all MGUE.

(20) In coordination with NSA, establish the security criteria for development and use of GPS UE for unattended and unmanned operations.

(21) Work with the Services in developing GPS UE to meet service unattended and unmanned operational requirements.

(22) Coordinate on any PPS devices included in FMS and DCS.

e. The SAASM KLIF will:

(1) Operate as the single government facility authorized to load all SAASM devices with the KDP operational software.

(a) The primary KLIF is located at Warner-Robins Air Logistics Center, GA.

(b) The alternate KLIF is located at Tobyhanna Army Depot, PA.

(c) All SAASM devices are processed at the KLIF during both the security design review and SAASM production processes. Processing at the KLIF is necessary to control access to and to ensure the security of the KDP operational software, supporting positive control of GPS security devices.

(2) Execute SAASM KLIF priority processing.

FOR OFFICIAL USE ONLY

(a) Priority processing (processing ahead of the standard first-in/first-out queuing procedure) of GPS security devices through the KLIF may be authorized in the interest of National Security.

(b) Priority processing requests must include the reason for the request, number of units to be processed and the required date (e.g., 30 June 2010).

(3) Notify NSA and the SMC/GP prior to non-standard KDP reprogramming.

(4) Execute SAASM KLIF contingency processing.

(a) Contingency processing may require the mobilization of KLIF hardware, software and personnel to support urgent programming or reprogramming requirements.

(b) When the mobile KLIF is required, users requesting support for contingency processing shall submit a SAASM KLIF contingency processing request through the appropriate COCOM or agency to USSTRATCOM. USSTRATCOM shall forward the request to Joint Staff/J-6, which will approve or deny the request. Joint Staff/J-6 will forward (approved) requests to the SMC/GP through HQ AFSPC, which will task the KLIF to respond.

(c) Mobile KLIF capabilities shall also be available to support routine programming or reprogramming requirements at forward and deployed locations where it is not feasible to return GPS Host Application Equipment (HAE) to the primary KLIF for reprogramming. Users requesting support for routine processing at forward or deployed locations shall submit a SAASM KLIF non-standard processing request through the appropriate COCOM or agency to USSTRATCOM. USSTRATCOM shall forward the request to Joint Staff/J-6, which will approve or deny the request. Joint Staff/J-6 will forward (approved) requests to the SMC/GP through HQ AFSPC, which will task the KLIF to respond.

(5) Maintain the alternate KLIF. The alternate KLIF is required to mitigate impacts of disasters (natural and man-caused) and will be activated when the Primary KLIF is inoperable and as required to exercise deployment capabilities. The Primary and Alternate KLIFs must operate with identical programming software configurations.

f. USSTRATCOM will:

(1) Implement and manage all applicable GPS security functions as defined by the SMC/GP and NSA.

FOR OFFICIAL USE ONLY

(2) Implement and manage the SAASM and MGUE keying material and key products required by the U.S. and Allied users (black keys, receiver initialization parameters, and BKA update parameters).

(3) Update and manage guidance documentation (i.e. CONOPS, etc.) to implement and execute GPS and NAVWAR Operations for the Warfighter.

(4) Implement and manage GPS black key crypto nets in the number and structure specified by the Joint Staff.

(5) Implement and manage the capability to execute emergency key supersession.

(6) Implement and manage the capability to approve delivery of GPS keying material to authorized GPS PPS users.

(7) Implement and manage the SAASM and M-Code navigation message bits as defined by the SMC/GP.

(8) Define the operational requirements for MNAV design and the proposed implementation and management for MNAV messages and provide to the SMC/GP for development and acquisition.

(9) Define the operational command and control requirements for SAASM and MNAV operations and provide to the SMC/GP for development and acquisition.

(10) Act as the GPS Key Material Controlling Authority.

(11) Coordinate KLIF contingency processing requests with the Joint Staff/J-6, NSA and the SMC/GP through HQ AFSPC.

g. The Services, COCOMs, and Agencies will:

(1) Ensure that users requiring non-standard (priority, contingency, etc.) processing at the KLIF submit a SAASM KLIF non-standard processing request through the appropriate COCOM or agency to USSTRATCOM. USSTRATCOM shall forward the request to Joint Staff/J-6, which will approve or deny the request.

(a) SAASM KLIF non-standard processing requests must include the reason for the request, the number of units to be processed, the date needed and a plan for compliance with applicable security requirements.

FOR OFFICIAL USE ONLY

(b) SAASM KLIF non-standard processing requests must have a planner-level (O-6 or GS/GM-15) signature before being forwarded to the Joint Staff/J-6 for validation and approval.

(c) Joint Staff/J-6 will forward (approved) requests to the SMC/GP through HQ AFSPC for action. If denied, Joint Staff/J-6 will provide an explanation to USSTRATCOM, who will forward the response to the sponsoring COCOM or Service.

(2) Ensure that systems requiring any SAASM reprogramming in the field provide an interface adapter (and path) capable of transferring data from the mobile KLIF to the KDP within the SAASM. The adapter will conform to requirements specified by the SMC/GP.

(3) Ensure that organizations, agencies and entities requiring use of the full-function SAASM simulator submit a request to the SMC/GP for approval.

(4) Ensure that SAEs and SPDs include the SMC/GP SAASM HAE approval requirements in each developer's DoD Contract Security Classification Specification, DD Form 254.

(5) Identify GPS UE requirements for unattended and unmanned operations and work with the SMC/GP to ensure GPS UE can meet those requirements.

FOR OFFICIAL USE ONLY

ENCLOSURE E

NAVIGATION WARFARE (NAVWAR)

1. Introduction. The DoD intends to gain and maintain PNT information superiority through the application of Navigation Warfare (NAVWAR) without unduly disrupting non-hostile PNT users outside an area of military operations. The elements to U.S. NAVWAR policy are:

a. Assure friendly use of PNT information.

b. Minimize interference to peaceful civil users of PNT information.

c. Deny adversary use of PNT information.

2. Definition. NAVWAR is defined in Joint Publication 3-13.1 Electronic Warfare as: "Deliberate defensive and offensive action to assure and prevent positioning, navigation, and timing information through coordinated employment of space, cyberspace, and electronic warfare operations."

3. NAVWAR Implementation. Military and civil users have grown dependent on assured PNT which is essential to effective joint operations and national critical infrastructure. At the operational-level, a Combatant Commander or Joint Force Commander (JFC) may gain a desired NAVWAR PNT information advantage by integrating diverse taskable NAVWAR capabilities, courses of action (COAs), and PNT effects. NAVWAR is necessary to ensure PNT information is available, accurate and reliable in electromagnetically contested (denied) and congested (degraded) environments, while also denying PNT information to an adversary. In the face of emerging anti-access/area denial strategies, NAVWAR capabilities and operations will become vital to gain PNT information superiority and an operationally relevant advantage (such as operational access) directly contributing to National Security Space Strategy objectives. Effective NAVWAR operations use asymmetric advantages and cross-domain synergy to achieve freedom of action across all mission areas, operational domains, and the full range of military operations (ROMO).

4. Central Ideas of NAVWAR. There are three central ideas to gaining PNT superiority in some combination of domains that will provide the freedom of action required by the mission.

a. Central Idea #1. *NAVWAR occurs in multiple environments, domains, and mission areas and typically involve PNT information from a variety of sources.* Commander, USSTRATCOM exercises command authority over NAVWAR mission areas, capabilities, and forces in support of JFCs. These mission areas

FOR OFFICIAL USE ONLY

include space operations, electronic warfare (EW) and, cyberspace operations, which organizationally reside within Joint Functional Component Command (JFCC) for Space (JFCC SPACE), United States Cyber Command (USCYBERCOM), and USSTRATCOM. Commanders (CDR) and their staffs will coordinate and synchronize the execution of space, cyberspace, and electronic warfare to assure friendly use of PNT information and, on order, to prevent or negate adversary use. This involves integrated offensive and defensive NAVWAR operations.

b. Central Idea #2.

(1) *NAVWAR operations require focused integration in planning, command and control (C2), and execution.* To achieve a PNT advantage, JFCs must integrate NAVWAR capabilities resident in multiple mission areas and functional processes to include space operations, cyberspace operations, electronic warfare, ISR, and joint electromagnetic spectrum operations. NAVWAR planning and execution is tailored to address anticipated conditions within the NAVWAR environment of a particular AOR. The coordination required to create NAVWAR effects involves various operations centers, as well as boards, bureaus, centers, cells, and working groups (B2C2WG).

(2) The President's Unified Command Plan (UCP) designates USSTRATCOM as the functional Combatant Commander (CCDR) for space, cyberspace, ISR, and EW capabilities. CDRUSSTRATCOM provides NAVWAR planning and execution support when requested by supported CCMDs and JFCs through a combination of standing reach-back capabilities at the Joint Functional Component Command for Space (JFCC SPACE) Joint Space Operations Center (JSpOC) and the Joint Navigation Warfare Center (JNWC) combined with forward deployed NAVWAR subject matter experts (SMEs).

c. Central Idea #3. *NAVWAR implementation requires materiel and non-materiel solutions across Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities and Policy (DOTMLPF-P).* A comprehensive DoD NAVWAR architecture will involve multiple domains and occupational specialties.

4. <u>GPS-Related NAVWAR Testing, Training and Exercises</u>. The Services must ensure that forces can operate in an intense EW environment. For this reason, DoD tests, training and exercises involving GPS jamming/interference are vital to the effective employment of combat forces. For more details, see CJCS Manual 3212.03, 15 December 2008 (Enclosure O, reference q).

FOR OFFICIAL USE ONLY

ENCLOSURE F

GPS USER EQUIPMENT ACQUISITION POLICY

1. GPS Equipment Status. Section 152(b) of the National Defense Authorization Act for Fiscal Year 1994 (Public Law 103-160; 107 Stat. 1578) placed limitations on procurement of systems not GPS equipped. This mandate, termed GPS 2000, prohibited obligation of funds to modify or procure any DoD aircraft, ship, armored vehicle, or indirect-fire weapon system not equipped with a GPS receiver after 30 September 2000. The National Defense Authorization Act for Fiscal Year 2005 (Public Law 108-375) extended the 30 September 2000 date to 30 September 2007. Public Law 111-383, section 913 states that the Department of Defense may not obligate funds to purchase user equipment for GPS during fiscal years after fiscal year 2017 unless the equipment is capable of receiving the military code (M-code) unless a waiver by the Secretary of Defense is granted. Equipping all affected DoD platforms is occurring at varying rates. Some DoD platforms are still equipped with legacy, red key only, GPS UE. However, many other platforms have either upgraded or are in the process of upgrading to black key capable SAASM UE.

a. SAASM generation cryptography offers more functionality than its predecessor, the legacy Precise Positioning Service Security Module (PPS-SM). As published in previous editions of this instruction, all newly fielded DoD systems will use SAASM-based GPS PPS receivers no later than 1 October 2006. DoD agencies that utilize legacy GPS PPS devices must provide their SAASM transition plan directly to OSD. Non-DoD agencies that utilize PPS are urged to comply with the spirit of this instruction. Waiver requests for non-SAASM equipment entering the field for combat, combat support or combat service support after 2006 shall be submitted from the Service Acquisition Executive (SAE) to OSD via the Joint Staff/J-6 IAW Paragraph D-3 and Enclosure K.

b. SAASM implements the Joint Staff and NSA requirement to transition the United States (and its allies) from classified red keys to unclassified black keys as soon as possible, as well as other significant NAVWAR related capabilities.

c. DoD SPS Use. There are a growing number of military users relying on SPS within the Department of Defense. Unauthorized SPS use undermines NAVWAR planning and efforts to implement new electronic protection capabilities to address GPS vulnerabilities. See Enclosure A and Enclosure D for more details on SPS use and SPS waivers.

FOR OFFICIAL USE ONLY

2. Acquisition Policy

a. The 7 August 2006 ASD(NII) memorandum, "Global Positioning System User Equipment Development and Procurement Policy," revised the previous GPS UE policy based on the significant advances in technology over the last decade. Technology is now enabling implementation of modular and software based GPS capabilities, embedding GPS receiver functionality into multi-purpose avionics systems and other platform electronics and personal/portable systems. The policy specifically articulates the GPS UE transition to the Military GPS Signal (M-Code) capable GPS UE (MGUE). Highlights of the revised policy are provided below:

(1) The SAEs for programs using GPS shall fund the development, integration and implementation of unique requirements not identified as common capabilities through the JCIDS process for GPS UE. They shall also fund procurement of production GPS UE.

(2) The Air Force, through the SMC/GP shall:

(a) Develop to production ready status form factors for the lead platforms identified by the Services, resulting from the JCIDS process. As additional common form factors are identified through the JCIDS process, the Air Force will POM for and develop those form factors.

(b) POM for and develop to production ready status common UE capable receivers to meet service needs as validated through the JCIDS process.

(3) MGUE capable equipment will be required for the following equipment categories not later than the date that the 24th M-Code satellite is declared operational:

(a) New Systems (pre-Milestone B) that require a military GPS capability shall implement a MGUE design.

(b) Existing Systems (post-Milestone B) and procurement of expendables shall prepare and present an implementation plan and funding of MGUE capability to OSD.

(c) Expendable Systems that are already in the inventory shall not be required to retrofit to MGUE capability.

FOR OFFICIAL USE ONLY

(d) Space Vehicles that are past integrated systems testing and vehicle thermal-vacuum testing and are ready for transportation to launch sites, shall not be required to retrofit to MGUE capability.

(e) Retiring Systems (out of DoD active and reserve inventory within 5 years) shall not be required to retrofit to MGUE capability.

FOR OFFICIAL USE ONLY

(INTENTIONALLY BLANK)

FOR OFFICIAL USE ONLY

ENCLOSURE G

PNT CAPABILITIES, SCIENCES AND TECHNOLOGIES

1. The DoD PNT Science and Technology (S&T) Roadmap is in its 3rd iteration. The S&T roadmap was developed by DUSD AT&L to coordinate and facilitate the development of DoD (PNT) capabilities through 2025. As such, it provides guidance for a coordinated S&T program to improve the PNT capabilities that support and enable DoD's emerging warfighter needs. It includes specific suggestions to address the PNT gaps identified in the 2006 PNT Joint Capabilities Document (Enclosure O, reference i) and for improving DoD coordination of PNT S&T activities. This should facilitate optimal use of limited PNT-related Research and Development (R&D) funds. DoD reliance upon PNT is often undocumented in the development of new communication, surveillance, targeting, logistic, weapon, or navigation systems. As a result, knowledge of potential system benefits of improved PNT capabilities may not be readily apparent to many in the acquisition community. The combination of this lack of knowledge and minimal coordination of PNT S&T efforts may lead to wasteful duplication of effort and/or unintentional degradation of essential future capabilities. The S&T Roadmap was developed for the following purposes:

a. To further focus DoD PNT S&T activities.

b. To provide a continuing plan for integration, synchronization, prioritization, and coordination of PNT development to meet DoD needs. This includes matching developing technologies with emerging threats to PNT.

c. To raise awareness in the acquisition community of potential system benefits derived from improved PNT capabilities – including non-GPS based approaches.

2. <u>S&T Roadmap Summary</u>:

a. The current Roadmap was signed in 2009. The next update is in draft.

b. PNT S&T Funding:

(1) Forty percent of funding levels for all PNT S&T programs are now allocated to integrated and autonomous systems.

(2) There remains a gap between Technology Readiness Levels (TRL) levels 3 and 7 for most PNT S&T efforts (with TRL 5 and 6 being the most difficult roadblocks to pass).

FOR OFFICIAL USE ONLY

c. Terrestrial-Based Radionavigation:

(1) Though there was little Medium and Low Frequency (MF/LF) type work forecasted in the 2006 roadmap, there is, nevertheless, a need for increased R&D in the MF/LF domains.

(2) There is a significant capability shortfall associated with navigation in underwater, indoor, urban canyon, and underground environments. There are several promising technologies which might address this gap, but they require more robust funding streams and leadership push.

d. Network Assisted GPS: Network Assisted GPS, tested as part of a 6.2 Advanced Technology assessment program, was determined to be beneficial in providing GPS ephemeris and ranging data.

e. Transition of Army PNT Technology:

(1) Micro-Electro-Mechanical System (MEMS). The Army's Common Guidance Common Sense (CGCS) program has successfully developed sufficiently accurate high-G MEMS IMUs for use in Army munitions. The Army's Digital Integrated GPS Navigation Unit (DIGNU) program has similarly supported the Army's tactical missiles.

(2) The Army's Advanced Pos/Nav and Tracking the Future Force program (a 6.2 research program) demonstrated the utility and improved performance obtainable from integrating multiple navigation sensors (e.g. GPS, Dead Reckoning Module, Doppler Sonar, IMU, and a standard Army radio into a single package). The resulting package provided accurate navigation in GPS-denied environments.

f. Orientation: GPS spacecraft attitude knowledge needs to be made accessible in a net-centric medium to achieve extremely precise positioning. This problem applies to non-GPS systems that will provide precision PNT solutions as well.

3. Action Taken

a. PNT S&T Roadmap Effectiveness. The roadmap:

(1) informed and influenced the development of USSTRATCOM's Functional Solutions Analyses (FSA) for PNT and Orientation.

(2) supported the National PNT Architecture study, and the PNT portion of the National Security Space Plan.

FOR OFFICIAL USE ONLY

(3) presented an Excel-based database of all PNT S&T programs in response to an OSD PNT S&T "data call."

(4) helped the service laboratories increase their coordination of PNT R&D activities and reduce duplication of efforts.

(5) enabled insight into the GPS Directorate's S&T portfolio for relevance to the DoD's Joint PNT missions.

b. Impact of the PNT S&T Roadmap on Funding: The roadmap activity has successfully defined new S&T directions and put new programs in place.

(1) The Chip-Scale Atomic Clock (CSAC) program was completed by Defense Advanced Research Projects Agency (DARPA) and transitioned to the Army. The Army is funding a manufacturing technology program to start mass producing the CSAC in the 2013 timeframe.

(2) Critical non-GPS PNT technologies were identified. These include:

(a) Terrain reference or terrain-aided navigation systems.

(b) Inertial Technology (e.g. hyper-precision, represented by laser cooled systems; ultra-reliable, affordable, high accuracy; low to medium performance).

(c) Stellar systems.

c. Database and terrain reference navigation work well for low to medium altitude airborne applications. Further investment is needed for development and integration of a Precision Terrain Aided Navigation (PTAN) sensor.

d. Terrestrial-Based Radionavigation. Navwar RDT&E MOU will investigate a multi-nation project to develop high sensitivity GPS and combined COM-NAV receiver. This was also identified in the PNT JCD.

e. Network Assisted GPS. This program is being incorporated by the Army into two prototype integrated navigation units under a new 6.3 development program.

f. Transition of Army PNT Technology:

(1) Programs such as the Common Guidance Common Sense (CGCS) and Army's Digital Integrated GPS Navigation Unit (DIGNU) have demonstrated

FOR OFFICIAL USE ONLY

the value of the S&T investment in MEMS IMU technology and suggest that further investment in this area is warranted.

(2) The Army has a current follow-on 6.3 development to the Advanced Pos/Nav and Tracking the Future Force program to reduce the size, weight, and power budget while simultaneously improving accuracy.

4. Positioning, Navigation, and Timing Assurance Initial Capabilities Document

(a) The United States Strategic Command (USSTRATCOM) PNT JCD identified gaps and redundancies in PNT capabilities for the joint warfighter and led to the identification of DOTMLPF solutions to these issues.

(b) The Army developed an Initial Capabilities Document (ICD) for PNT Assurance in April of 2010. PNT assurance capability gaps identified in the JCD and associated DOTMLPF solutions are summarized and prioritized in this ICD (Enclosure O, reference r). The ICD also defines required PNT Assurance operational capabilities through 2025, with the capacity for future growth. It describes the PNT Assurance requirements for the Joint Operating Concepts and Joint Functional Concepts as well. There is no single PNT system that can meet all the needs and operational requirements of warfighters and the Joint Force (JF). As a result, the current DoD PNT architecture consists of a multitude and mix of different PNT systems. For instance, GPS alone cannot provide precise PNT capability in sub-surface and other impeded conditions. In benign and NAVWAR environments, a JFC should be able to access a variety of methods and capabilities to ensure access to precise PNT. The tasks, standards and conditions to assure warfighter access to PNT information are identified in this ICD as PNT Assurance.

(c) The GPS Enterprise Modernization and PNT Assurance AoA (GPSEM AoA) addresses future PNT assurance issues and directs the services to consider specific technical solutions in the acquisition of GPS equipment and systems.

FOR OFFICIAL USE ONLY

ENCLOSURE H

CONTROL OF PNT SERVICES IN TIMES OF TENSION OR WAR

1. The National Security Act of 1947 and Executive Order 11490 direct the Department of Defense (in partnership with DOT) to develop plans for the control of civil and military air traffic during national defense emergencies. In compliance with these directives, the North American Aerospace Defense Command (NORAD) and U.S. Pacific Command (USPACOM), in concert with DOT/FAA and DHS/TSA, establish policy and responsibilities for the control of air traffic during such emergencies. This policy is known as Emergency Security Control of Air Traffic (ESCAT). ESCAT replaced the older Security Control of Air Traffic and Air Navigation Aids (SCATANA). ESCAT facilitates control of specified airspace during national defense situations. ESCAT does not facilitate or call for the shutdown of PNT or ground-based Navigational Aids (NAVAIDS). If such plans are deemed a requirement, these plans shall be developed outside of the ESCAT Plan.

2. GPS and Augmentations (DGPS). It is U.S. national policy to provide SPS signals free of the intentional degradation known as Selective Availability (SA). The United States has no intent to ever employ SA again. The current constellation, however, still retains the capability to degrade SPS signals through SA. The employment of SA may be authorized only by the President of the United States (POTUS). Requests to employ this capability must originate from a COCOM and be submitted through USSTRATCOM for validation by CJCS. The decision to employ SA rests solely with the POTUS. If time and circumstances permit, the Department of Defense will consult with the Secretaries of Transportation and Homeland Security before implementing SA. Civil users will be notified via Notice to Airmen (NOTAM) and Notice to Mariners (NOTMAR) in this case. GPS III will be built without SA capability.

3. The Communications Act of 1934 (Title 47, U.S.C., section 606, as amended) authorizes the President, during times of national emergencies or war, to exercise extraordinary management and control of virtually every form of telecommunications resource at the national and local levels. This includes all frequency and spectrum resources in the United States and its territories. Executive Order 11490 directs the Department of Defense (in partnership with the FCC) to develop plans and programs for the emergency control of all devices capable of emitting electromagnetic radiation.

FOR OFFICIAL USE ONLY

(INTENTIONALLY BLANK)

FOR OFFICIAL USE ONLY

ENCLOSURE I

GEOSPATIAL INFORMATION AND SERVICES

1. Purpose. The purpose of this enclosure is to describe, in general terms, the capability and limitations of Geospatial Information and Services (GI&S) products and their relationship with GPS.

2. Background

a. GI&S products, in some form, have been an integral part of every navigation system and must be linked by a common reference system. Historically, horizontal and vertical reference systems have been determined independent of one another. Horizontal reference systems have usually been local or regional and non-geocentric. Vertical positions have been referenced to an equipotential surface that approximated mean sea-level.

b. The use of space-based PNT systems makes the determination of three-dimensional coordinates related to a common geocentric reference routine. The common reference system used by GPS is the WGS 84. GPS is the primary means by which users obtain coordinates referenced to WGS 84. NGA provides the defining WGS 84 parameters as well as datum shift constants, coordinate transformation formulas, gravity potential coefficients, geoid model, and a magnetic model. NGA, as the lead agency for all DoD geodetic reference systems and GI&S products, is responsible for ensuring continuous compatibility with GI&S products.

3. Accuracy Objectives. GPS accuracy requirements impose rather stringent positional accuracy demands on both navigation systems and GI&S products used for mission planning, rehearsal, and execution. All GI&S products do not exhibit the same level of absolute and relative accuracy. Some products such as the digital point positioning database (DPPDB) are designed to support the accuracy requirements of precision guided munitions, while topographic maps serve a different purpose. Users must choose the appropriate set of GI&S products that support their mission objectives.

a. Absolute accuracy of maps and charts is dependent on the accuracy of the geodetic control network upon which those maps and charts are based. The most commonly used maps, the 1:50,000 scale maps, are generally built to a 50 m (Cat II/B), 90 percent circular probability standard, relative to ground control.

b. Although maps and charts are traditional GI&S navigation support products, other GI&S products such as DPPDB, digital vertical obstruction file

FOR OFFICIAL USE ONLY

(DVOF), digital aeronautical flight information files (DAFIF), digital terrain elevation, and digital feature analysis data (DFAD) also provide required geodetic positions. A precise accurate point positioning database derived using photogrammetrics in conjunction with validated imagery mensuration tools and algorithms can provide precise position and elevation as required by national priorities, policies, and doctrines.

4. Worldwide Positioning

a. WGS 84 provides a common accessible global reference frame for DoD operations. NGA GI&S products and other geospatial data generated within the Department of Defense use WGS 84 to the maximum extent possible as the global framework (datum) for these products and all DoD operations. This geocentric reference frame uses the center of mass of the Earth as the origin and closely follows international conventions regarding the scale and orientation of the reference frame axes.

b. For many reasons, global geocentric reference frames such as WGS 84 have been adopted rapidly in disciplines such as geodynamics, geodesy, and satellite operations. In contrast, some mapping organizations around the world must deal with the labor-intensive process associated with conversion of existing maps to a modern geocentric reference frame (datum). Many existing maps and nautical charts were created with legacy processes that typically used non-geocentric, regional geodetic data that differ from WGS 84, in some cases, by several hundred meters.

c. To allow use of these older mapping products generated on regional data, transformation parameters have been developed that allow a cartographer or other user to convert geospatial data represented on a regional geodetic datum to WGS 84. However, most of these transformation parameters exhibit uncertainties in the range of 2 and 25 m. This level of accuracy may be adequate for some mapping applications, but a significant amount of care must be exercised before a datum transformation is used in an application that requires a specific level of geospatial accuracy. In some cases, datum transformations may not even be available.

d. Until all maps are referenced to WGS 84, there will be a need in the U.S. government for accurate transformation parameters between WGS 84 and local datums. Until this goal is achieved, a need for these datum transformations will persist and users must be aware of the accuracy limitations associated with the datum transformation process.

e. The WGS 84 is consistent within its precision with the International Terrestrial Reference Frame maintained as the international standard by the International Earth Rotation Service. NGA ensures that WGS 84 is compatible

FOR OFFICIAL USE ONLY

with other global geodetic reference systems, which contributes to GPS compatibility with foreign GNSS.

5. GI&S Data Acquisition. The implementation of GPS has greatly expanded the GI&S positioning capability by providing a means by which worldwide geodetic control networks can be developed. The increased density of geodetic control allowed by GPS can be used to improve target and fix-point databases to meet expected weapon system requirements.

6. Products. Use of graphic products in support of present navigation systems will be largely replaced in pending systems by the use of modernized, standardized digital GI&S data. As systems are developed, digital (and other), GI&S requirements should be addressed as early in the process as possible to ensure that GI&S support will be available when the system is implemented. Users may continue to require graphics to maintain orientation in case of system failure or to predict a passage between digitally recorded points. The requirements for graphics will continue to be satisfied by both mono and stereo controlled imagery such as orthophotos and DPPDB, as well as other forms of visual representation that portray position in terms of the navigation system coordinate readouts.

7. Artillery Point Positioning. Precision targeting area accuracies available with the GPS broadcast signal, supplemented by the emerging near-real-time precision GPS, will continue to expand the GI&S capability in providing timely, accurate positional information necessary to support precision artillery and mortar fires. Artillery positional requirements exist for firing batteries, counter-mortar radars, other target location sensors, and forward observers.

8. Bathymetry, Gravity and Geophysical Data. Another application of GPS as a GI&S resource is in the collection of bathymetric, gravimetric and other geophysical data (e.g. magnetic, seismic, geologic). In the past, surveying of bathymetric, gravimetric and other geophysical features required the use of non-satellite based navigation systems. These may have involved labor intensive geodetic surveying or low accuracy map scaled positioning techniques. GPS permits rapid, accurate positioning of bathymetric features, by survey ships in all ocean areas, as well as accurate positioning of gravimetric and other geophysical feature locations. Accurate bathymetry enables improved surface ship and submarine navigation and ocean current models. Accurate gravity and magnetic products are used in military navigation systems.

9. Multi-sensor Aerial Mapping. Currently, GPS broadcast signal augmented by differential techniques (i.e. CORS) provides airborne sensor platforms with positioning accuracies that meet the error allowed for production of large-scale topographic maps within a few days of image capture. Currently these

FOR OFFICIAL USE ONLY

accuracy levels can only be met by using electronic navigation systems that have a limited range and therefore limit efficiency and potential area coverage. GPS, augmented with a near real time precision GPS signal, will exceed the accuracies required for large-scale topographic mapping within targeting timelines and deliver that capability worldwide.

10. Limitations of Traditional GI&S Products. Traditional paper products (maps and charts) are not intended to be used for precise positioning and cannot give accurate positions no matter how carefully features are measured. The scale of the product, the survey control methods used, the mapmaking standards applied, and the symbolization of features all limit the possible accuracy attainable for the product. Digital products derived from traditional map sources (i.e. digitized) are of the same quality as their paper product sources. Although digital products made directly from imagery sources are still not perfect and are affected by production standards applied, they eliminate the other errors noted above and provide the most accurate positions.

11. Future Product Needs. As more sophisticated uses of PNT are developed, increased demand and more stringent requirements are being levied on GI&S products. These higher accuracy requirements include: improved (near-real-time) satellite modeling; enhanced WGS 84 Earth Gravity models, and more precise geodetic control. GPS is key to providing enhanced absolute accuracy for weapons, improved relative and absolute positioning and significantly reduced mission planning time. NGA plans to provide data that supports precision navigation and targeting in a GPS degraded environment beginning in FY14. NGA continues to develop methods and techniques to provide timely, relevant, and accurate GI&S products that support National Space Policy, National Cyber Policy, and Joint Vision 2020. NGA is transforming to an on-line and on-demand environment to meet the needs of users.

12. Time-Space-Position Information (TSPI). Unambiguous specification and implementation of Time-Space-Position Information (TSPI) is central to Geospatial Intelligence (GEOINT) and the functioning of the National System for Geospatial Intelligence (NSG) and the Allied System for Geospatial Intelligence (ASG), NATO and all partners. The National Geospatial-Intelligence Agency (NGA) GEOINT manager is a key stakeholder in ensuring that TSPI implementation is well-specified – particularly for precise spatiotemporal positioning for the purposes of targeting and safe navigation. Not all communications of TSPI data, today, include explicit characterization of their spatiotemporal reference system(s). This TSPI specification provides a “bridge” from legacy information exchanges (e.g., USMTF and VMF-XML) to a well-structured, well-documented, robust eXtensible Markup Language (XML) schema developed for spatiotemporal data which has broad DoD and Intelligence Community (IC) applicability. Standardized TSPI schema supports a broad range of existing and future business practices for time-space-position

FOR OFFICIAL USE ONLY

information specification and exchange within all elements of the NSG, ASG, NATO and our partners. All participants to the TSPI exchange must communicate how differing spatiotemporal reference systems relate to the "real Earth" (e.g., the relationship between Military Grid Reference System (MGRS) "flat" coordinates and geodetic coordinates on a "curved Earth"). As the promulgating Agency for MGRS and WGS 84, NCGIS/NGA has issued this TSPI standardization practice, to address community interoperability by adoption and support of TSPI for GEOINT within DoD/IC systems across the NSG, ASG and our partners. This specification is contained within the NGA Standardization Document: Time-Space-Position Information (TSPI), STND.0019, Version 2.0, dated 2012-04-05.

FOR OFFICIAL USE ONLY

(INTENTIONALLY BLANK)

FOR OFFICIAL USE ONLY

ENCLOSURE J

PRECISE TIME AND TIME INTERVAL (PTTI)

1. Introduction. Timing services, with various degrees of precision, are required by numerous systems and support many critical missions. Radio electronic navigation, secure communications, electronic surveillance, improved identification, collision avoidance, formation flight, ATC, missile operations, satellite geodesy, and sun-tracking systems are examples of systems and missions that use precise clock time and frequency synchronization. This enclosure discusses PTTI and its importance to military operations. Additionally, with the emphasis on network-centric operations and the global sharing of information, there can only be one time standard to synchronize all systems. This time standard is the Master Clock maintained at the U.S. Naval Observatory (USNO).

2. Responsibilities. The USNO, Washington, DC, is the agency, designated by the Department of Defense, responsible for PTTI reference values for all Services, agencies, contractors, and related scientific laboratories, coordinating DoD timing capabilities, analysis, evaluation, and monitoring of Research and Development (R&D) and operational PTTI systems. The Superintendent USNO is the DoD PTTI manager. The USNO accomplishes its mission by maintaining a master clock (MC) timing facility in Washington, D.C., and an alternate master clock (AMC) facility, designated USNO AMC, at Schriever Air Force Base, Colorado.

3. Requirements

a. Most timing requirements are based on a need for synchronization or coordination among cooperating units of a system or between systems. Although synchronization is maintained internally in some systems, others must acquire synchronization independently before participating in system activities. For these and for platforms that must operate with other precisely timed systems, a common, accessible standard is needed. The standard for military systems is UTC (USNO), as maintained by the USNO Master Clock, UTC (USNO).

b. Time accuracy is the degree to which UTC (USNO) is known or maintained by systems requiring interoperability. In GPS, the accuracy of the delivered UTC (USNO) is affected both by GPS space vehicle (SV) onboard clock timekeeping ability and the frequency with which the SV clocks can be periodically updated through UTC (USNO) dissemination services. Most military electronic systems require a precise and accurate common time, which is the reference time as established by the USNO. Accuracy requirements vary

FOR OFFICIAL USE ONLY

among systems, nevertheless, a means of referring system clocks to the Department of Defense time reference is necessary.

c. Uses of a precise time scale vary greatly for civil and military users. Timing accuracy requirements vary widely depending on the nature of each use. Celestial navigation requires timing accuracy of 0.1 second (one sigma). One to 100 milliseconds (one sigma) are required for wide area computer networks, and future high speed networks could soon require microsecond accuracy. One hundred microseconds (one sigma) are required for some geodetic and geophysical applications, missile technology, and satellite observations. One-sigma accuracies ranging from minutes to five nanoseconds or less (synchronized clock time) are required for DoD applications. Specific time and frequency requirements for other radionavigation systems may be obtained from the USNO. Precise time can be considered a utility with virtually the entire population being affected by some degree of timing requirement.

d. Astronomical time (UT1) of 100 microsecond accuracy is provided by USNO to users requiring access to inertial reference frames for targeting, satellite orbit determination, navigation, and geodetic applications. There are several thousand military and civilian users having this requirement.

e. Ten nanoseconds synchronized clock time is currently the most stringent timing requirement for DoD operational applications. Proponents of space research, radio astronomy, and advance time system development have requested sub-nanosecond level accuracy.

4. Current Operations. Users may acquire precise time information to address their requirements from a variety of sources that are traceable to USNO. Figure J-1 highlights some commonly used techniques. Methods of receiving PTTI are described below:

		RMS Accuracy	
System	Mode	Specification	Typical
GPS PPS	Passive	20ns	8ns
GPS SPS	Active	20ns	16ns
TWSTT	Active	5ns	1 to 3ns
Voice Announcer	Active	1s	.5s
Modem	Active		1ms
NTP	Active	50ms	10 to 50ms

Figure J-1. Systems Distributing UTC (USNO)

a. The most common means by which most DoD users obtain UTC (USNO) is through the dissemination of time by the GPS constellation. Some operators may refer to this time as GPS time because it is delivered by GPS, but it is in

FOR OFFICIAL USE ONLY

fact UTC (USNO) being received (within the accuracy limits of the GPS receiver). Therefore, personnel using GPS will normally be synchronized with the USNO Master Clock and with each other.

NOTE: Care must be taken to distinguish UTC (USNO) obtained from GPS from the internal GPS system time which is offset by integral seconds from UTC (USNO). Operators and acquisition developers should not use the internal GPS system time for operational timing as this will hinder interoperability and may prevent the proper operation of communications and intelligence systems.

b. USNO provides certification of clocks or systems involved in time dissemination, weapons integration, surveillance, countermeasure systems coordination, and satellite control. This certification is accomplished by providing documentation of traceability to UTC (USNO).

c. TWSTFT (Two-Way Satellite Time and Frequency Transfer) is available from USNO for high-precision PTTI. This procedure makes use of geostationary communications satellites to transfer time. The level of accuracy depends on the user's situation. If the TWSTFT system is calibrated, one nanosecond time transfer is possible. USNO provides a calibration service using this TWSTFT technique supporting user systems with the most stringent timing requirements.

d. USNO provides a voice time announcement and time ticks (accurate to the millisecond level if propagation delays are known from a previous measurement). See Figures J-2 and J-3.

e. The USNO provides computer network time synchronization service meeting Internet standard RFC-1305 NTP. USNO NTP servers provide UTC (USNO) with millisecond accuracy over wide area networks, including the Non-Secure Internet Protocol Routing Network (NIPRNET) and SIPRNET.

TELEPHONE VOICE TIME ANNOUNCER	**TELEPHONE TIME FOR COMPUTERS**	**TIME OVER THE INTERNET and SIPRNET**
(202) 762-1401 DSN 762-1401 or (719) 567-6742 DSN 560-6742	(202) 762-1594 DSN 762-1594 or (719) 567-6743 DSN 560-6743 1200 Baud, No Parity, 8 Bit	Via Network Time Protocol:

FOR OFFICIAL USE ONLY

Figure J-2. Sources of USNO Time

Servers are geographically dispersed to minimize network delay and distribute traffic. These 'Stratum One' level NTP servers are synchronized to UTC (USNO) through either direct connection to the Master Clock or through remote servers synchronized to UTC (USNO) as transmitted by GPS.

DATA VIA MODEM	DATA OVER THE INTERNET
(202) 762-1602 (202) 762-1610 (202) 762-1503 1200 - 14400 Baud No Parity 8 Bit	Via Telnet: tycho.usno.navy.mil Login: *ads* Via World Wide Web: http://www.usno.navy.mil/USNO/time Via Anonymous FTP: tycho.usno.navy.mil Login: *anonymous* Password: *your e-mail address*

Figure J-3. Sources of USNO Information and Data

5. Other Issues

a. NATO has produced a Military Operational Requirement for the Provision of Precise Time (MMC-SFM-081-93) dated 28 July 1993. This document has three main provisions: (1) the adoption of an agreed source as precision time reference; (2) the dissemination of the time reference; and (3) the acquisition and maintenance of the precise time reference with the appropriate level of accuracy. The reference was approved as UTC, but the other provisions will require the definition of architecture to describe how the various systems will interoperate in order to maintain the accuracies necessary for the different users and systems requirements.

b. The interface between USNO and GPS is specified by the interface control document ICD-GPS-202 that states that GPS time must be maintained within one microsecond of UTC (USNO). There is a further requirement that the transmitted UTC (USNO) must be within 28 ns of UTC (USNO).

c. The Navy continues to upgrade the Master Clock System at USNO to achieve an order of magnitude improvement in frequency stability to below one

FOR OFFICIAL USE ONLY

part in 10^{15}. This time reference system will be used for both current and projected user systems with PTTI requirements.

6. Leap Seconds

a. Historically, the second was defined in terms of the rotation of the Earth as 1/86,400 of a mean solar day. In 1967, the second was defined in terms of atomic time in the International System of Units (SI) as the duration of 9,192,631,770 periods of the radiation corresponding to the transition between the two hyperfine levels of the ground state of the cesium 133 atom.

b. International Atomic Time (TAI) is a statistical atomic time scale based on a large number of clocks operating at standards laboratories around the world that is maintained by the Bureau International des Poids et Mesures (BIPM); its unit interval is exactly one SI second at sea level. It was once recommended by the BIPM that systems which cannot handle leap seconds use TAI instead.

c. UT1 is the time based on the Earth's rotation. UTC differs from TAI by the total number of leap seconds, so that UT1-UTC stays smaller than 0.9s in absolute value. The decision to introduce a leap second in UTC is the responsibility of the International Earth Rotation and Reference System Service (IERS). Since leap second adjustments were introduced in 1972, all leap seconds have been positive. Twenty five leap seconds have been added as of June, 2012. This pattern reflects the general slowing trend of the Earth.

d. The starting epoch for GPS System Time is January 6, 1980. GPS Time is NOT adjusted for leap seconds. As of July 1, 2012, GPS is ahead of UTC (USNO) by 16 seconds. For GPS, the leap second correction contained within the UTC data of subframe 4, page 18 of the navigation message transmitted by satellites will change appropriately. GPS receivers built in accordance with ICD-GPS-200 should adjust for this leap second change without user intervention and the change should be transparent to the user.

e. USNO, USSTRATCOM, USCG and FAA will make notifications of leap second adjustments to various civilian and military information and control centers where management of user issues takes place.

7. Backup Capability. If, for any reason, the Washington facility of USNO is incapacitated, UTC (USNO) dissemination functions will be transferred automatically to the AMC facility at Schriever AFB, Colorado. A plan for a Distributed Master Clock is being developed to meet future requirements. It is anticipated that this system will consist of a series of Precise Time Stations, having reference clocks traceable to UTC (USNO).

FOR OFFICIAL USE ONLY

(INTENTIONALLY BLANK)

FOR OFFICIAL USE ONLY

ENCLOSURE K

WAIVER REQUEST PROCESS FLOW CHART

Waiver requests shall be addressed to:

Joint Staff/J-6 DD Cyber/C4 Transport Division – Space Branch
Pentagon, Room 1C1042
Washington, DC 20318-6000
ATTN: Space Transport Branch

Email: NIPR Organizational email: js.pentagon.j6.mbx.ddc4-pnt@mail.mil
SIPR Organizational email: js.pentagon.j6.mbx.ddc4-pnt@mail.smil.mil

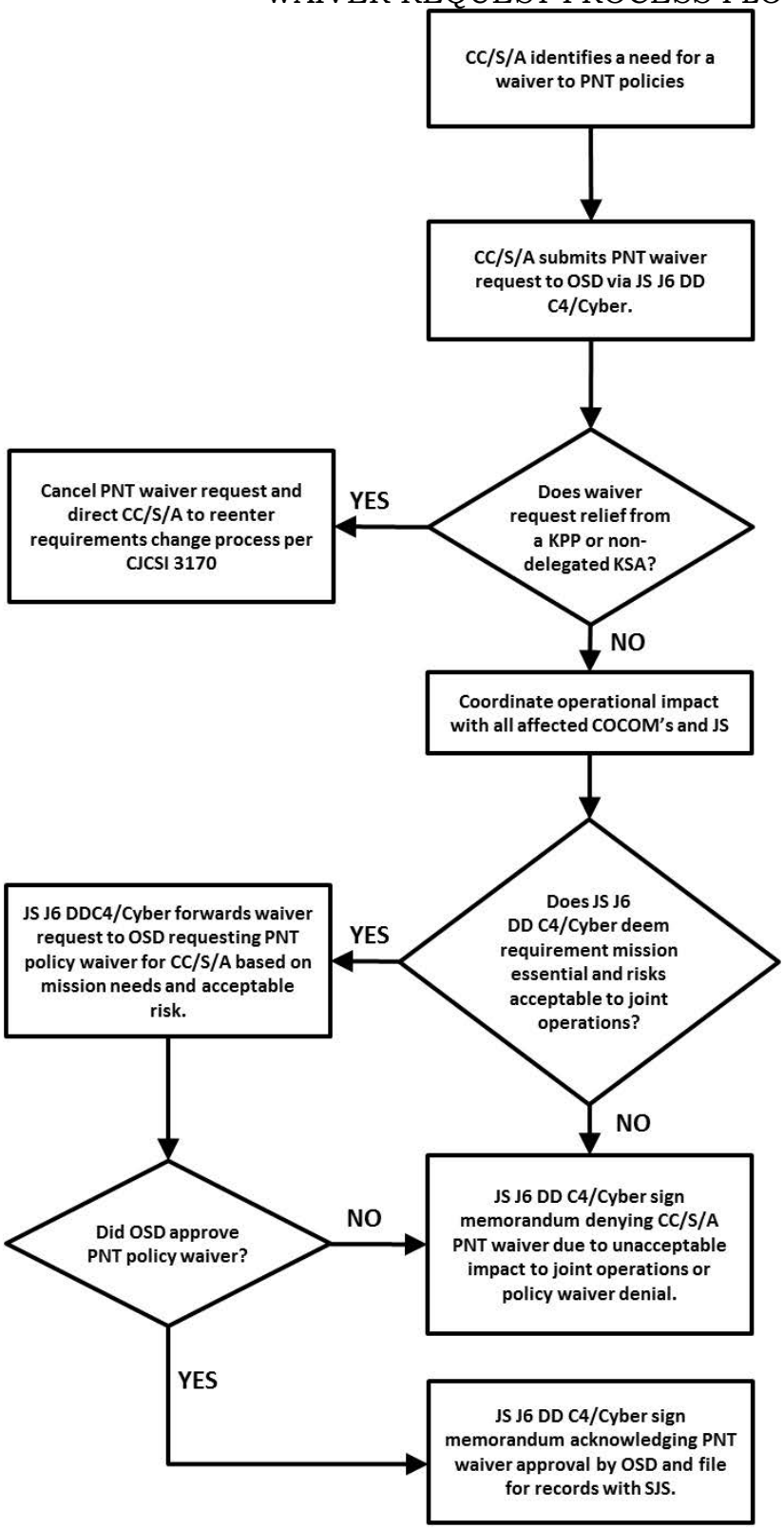
Waiver requests shall include the following essential information:

1. SPS Waiver Request
   - Reason(s) for non-compliance
   - Quantity (by device and platform)
   - Fielding plan
   - Compliance plan
   - Denial and spoofing risks
   - Risk mitigation plan
   - Capability statement
   - Source of the requirement
   - System KPPs and KSAs
   - Impact of waiver on achieving KPPs/KSAs
   - Statement of risk understanding & mitigation
   - Requirements Authority acceptance of Risk
   - CCMD notified and limiting factors noted in plans where system to be Assigned/ Apportioned/ Allocated/Attached

2. Waiver Request for U.S. Legacy PPS
   - Reason(s) for non-compliance
   - Quantity (by device and platform)
   - Lifecycle
   - Sustainment plan
   - Compliance plan
   - Crypto key support – type and duration
   - Contingency Recovery risk understanding/mitigation
   - Projected Foreign Sales?
   - CCMD notified and limiting factors noted in plans where system to be Assigned/ Apportioned/ Allocated/Attached

FOR OFFICIAL USE ONLY

WAIVER REQUEST PROCESS FLOW CHART



FOR OFFICIAL USE ONLY

ENCLOSURE L

PNT WAIVER REQUEST FORMAT EXAMPLE

[Service Letterhead]
MEMORANDUM FOR OFFICE OF THE SECRETARY OF DEFENSE

FROM: [originator and address]

VIA: JOINT STAFF/J-6 DDC4/CYBER

SUBJECT: Request for a PNT Precise Positioning Service (PPS) Waiver

1. In accordance with 2013 CJCS Master Positioning, Navigation, and Timing Plan (MPNTP) 6130.01E, request you waive the PPS requirement for the following program [state the program]. Waiver request for the [state the program] is submitted due to [state the reason for the request IAW Enclosure K].

2. Use of Standard Positioning Service (SPS) in the [state the program] results in limited or no reduction in mission capability of the host platform (or system) when operating in a jammed or other electronically challenged environment.

3. Affected Key Performance Parameters (KPPs) and Key System Attributes (KSAs) are [state affected KPPs and KSA].

4. The risk associated with the use of SPS for this program has been assessed and acknowledged. The CCMD(s) where this system will be employed has been notified. I accept the associated risks.

NAME
General/Flag Officer, Service
Signature Block

Attachment:
As stated

FOR OFFICIAL USE ONLY

(INTENTIONALLY BLANK)

FOR OFFICIAL USE ONLY

ENCLOSURE M

PNT WAIVER REQUEST APPROVAL

THE JOINT STAFF
WASHINGTON, DC

Reply ZIP Code:
20330-0600

MEMORANDUM FOR OFFICE OF THE SECRETARY OF DEFENSE

SUBJECT: Request for a PNT Precise Positioning Service (PPS) Policy Waiver

1. CC/S/A has requested a waiver to the PPS requirement, in accordance with 2013 CJCS Master Positioning, Navigation, and Timing Plan (attached).

2. The Joint Staff reviewed this waiver request and has determined that the requirement is essential to mission success, and any impacts do not pose unacceptable risks to joint operations. The Joint Staff recommends approval of this waiver request.

3. My point of contact for this matter is [POC name]. He/She can be reached at [phone number, DSN [phone number].

NAME
Brigadier General, USAF
Deputy Director for Command, Control, Communications, and Computers/Cyber, J-6

Attachment:
As stated

FOR OFFICIAL USE ONLY

DoD CIO Decision:
Approved _____
Disapproved _____

USD(AT&L)
Approved _____
Disapproved _____

FOR OFFICIAL USE ONLY

ENCLOSURE N

PNT PPS WAIVER DENIAL

THE JOINT STAFF
WASHINGTON, DC

Reply ZIP Code:
20330-0600

MEMORANDUM FOR COCOM/Service/Agency

Subject: PNT Precise Positioning Service (PPS) waiver request denied

1. Your request to waive the PPS requirement for PNT systems has not been sent forward to the Office of the Secretary of Defense due to [reason for denial].

2. My point of contact for this matter is [POC name]. He/She can be reached at [phone number, DSN [phone number].

NAME
Brigadier General, USAF
Deputy Director for Command, Control,
Communications, and
Computers/Cyber, J-6

cc:
DoD CIO
USD(AT&L)

FOR OFFICIAL USE ONLY

(INTENTIONALLY BLANK)

FOR OFFICIAL USE ONLY

ENCLOSURE O

REFERENCES

a. DOT-VNTSC-RITA-08-02/DoD-4650.5, "2010 Federal Radionavigation Plan"

b. DoD Global Positioning System Security Policy, 4 April 2006

c. DoD Directive 4650.05, 19 February 2008, "Positioning, Navigation, and Timing"

d. DepSecDef memorandum, 12 July 2012, "Recommendation for the Future Designation of the OSD Principal Staff Assistant (PSA) for Positioning, Navigation, and Timing (PNT) (OSD001790-12)"

e. DoD Global Positioning System Security Policy, 4 April 2006

f. "Global Positioning System Standard Positioning Service Performance Standard," September 2008

g. National Security Presidential Directive, Number 39 (NSPD-39), 8 December 2004, "U.S. Space-Based Positioning, Navigation, and Timing Policy"

h. DoD Instruction 4650.06, 24 November 2009, "DoD Positioning, Navigation, and Timing Executive Committee and Working Groups"

i. Joint Capabilities Document for Positioning, Navigation, and Timing, 26 September 2006

j. Capability Development Document for Global Positioning System III, November 2011

k. JROCM 152-09, 16 September 2009, "Global Positioning System III Increment A for KDP-C"

l. CJCSI 6510.06 series, 18 December 2006 (Current of January 2008), "Communications Security releases to Foreign Nations"

m. DoD Instruction 4650.07, 23 November 2011, "Precise Time and Time Interval (PTTI)"

n. GPS SAASM Concept of Operations, 13 October 2005

o. "GPS Cryptographic Key Ordering Instructions for Precise Positioning Service Users," 17 March 2011

FOR OFFICIAL USE ONLY

p. Selective Availability Anti-Spoofing Module Cryptonet Architecture Transition Plan, 16 September 2005, Change 2

q. CJCS Manual 3212.03 series, 15 December 2008, "Performing Tests, Training, and Exercises Impacting The Global Positioning System (GPS) In The United States and Canada"

r. Initial Capabilities Document for Positioning, Navigation, and Timing Assurance, April 2010

FOR OFFICIAL USE ONLY

GLOSSARY

ADS	Automatic Dependent Surveillance
AFB	Air Force Base
AFSPC	Air Force Space Command
A/J	Anti Jam
AMC	Alternate Master Clock
AMCS	Alternate Master Control Station
AS	Anti-Spoof (GPS)
ASD	Assistant Secretary of Defense
ASG	Allied System for Geospatial Intelligence
AT	Anti-Tamper
ATM	Air Traffic Management
BCVm	Black Crypto Variable Monthly
BIPM	Bureau International des Poids et Mesures (i.e., *International Bureau of Weights and Measures*)
BKA	Black Key Algorithm
BMCS	Back-Up Master Control Station
BGUV	Black Group Unique Variable
C/A	Coarse/Acquisition (GPS signal)
C4	Command, Control, Communications, and Computers
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CCMD	Combatant Command
CBA	Capabilities Based Analysis
CDRUSSTRATCOM	Commander, U.S. Strategic Command
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CNET	cryptographic network
CNO	Chief of Naval Operations
CNS	Communications, Navigation, Surveillance
COCOM	Combatant Command (Command Authority)
CONOPS	Concept of Operations
CRAF	Civil Reserve Air Fleet
CRF	Celestial Reference Frame
crypto	cryptographic
DAFIF	digital aeronautical flight information file(s)
DARPA	Defense Advanced Research Projects Agency
DAS	Defense Acquisition System
DCS	Direct Commercial Sales
DFAD	digital feature analysis data

FOR OFFICIAL USE ONLY

DGPS	Differential Global Positioning System
DHS	Department for Homeland Security
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoD CIO	Department of Defense Chief Information Office
DOT	Department of Transportation
DPPDB	digital point positioning database
DTED	digital terrain elevation data
DVOF	digital vertical obstruction file
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership (and Education), Personnel and Facilities
EMP	Electromagnetic Pulse
EMS	Electromagnetic Spectrum
EP	Electronic Protection
ESCAT	Emergency Security Control of Aircraft
ESG	Executive Steering Group
EXCOM	Executive Committee
FAA	Federal Aviation Administration
FMS	Foreign Military Sales
FRP	Federal Radionavigation Plan
FY	Fiscal Year
FYDP	Future Year Defense Program
GA	Ground Antenna
GATM	Global Air Traffic Management
GI&S	Geospatial Information and Services
GPS	Global Positioning System
GPSOC	GPS Operations Center
SMC/GP	GPS Directorate
GUV	Group Unique Variable
HAE	Host Applications Equipment
HQ	Headquarters
Hr	hour
Hz	hertz
IA	Information Assurance
ICAO	International Civil Aviation Organization
ICD	Interface Control Document Initial Capabilities Document
ILS	Instrument Landing System
IMO	International Maritime Organization

FOR OFFICIAL USE ONLY

INS	Inertial Navigation System
IS	Interface Specifications
JCD	Joint Capabilities Document
JCIDS	Joint Capabilities Integration & Development System
JEWC	Joint Electronic Warfare Center
JFC	Joint Force Commander
JFCC	Joint Functional Component Command
JIOWC	Joint Information Operations Warfare Center
JMAPS	Joint Milli-Arcsecod Pathfinder Survey
JNWC	Joint Navigation Warfare Center
JPALS	Joint Precision Approach and Landing System
JROC	Joint Requirements Oversight Council
JROCM	JROC Memorandum
JS-DSE	Joint Staff Decision Support Environment
JSpOC	Joint Space Operations Center
JV	Joint Vision
KDP	Key Data Processor
KLIF	Key Data Processor Loading and Installation Facility
km	kilometer
KMI	Key Management Infrastructure
KPP	Key Performance Parameter
kW	kilowatt
LAAS	Local Area Augmentation System
m	meters
M-Code	Military Code
MCS	Master Control Station (GPS)
MEMS	Micro-Electro-Mechanical Systems
MGUE	Military GPS User Equipment
MHz	megahertz
MF/LF	Medium Frequency/Low Frequency
MLS	Microwave Landing System
MNS	Mission Needs Statement
MPNTP	Master Positioning, Navigation, and Timing Plan
MS	Monitor Station
MURI	Multi-University Research Initiative
NAS	National Airspace System
NATO	North Atlantic Treaty Organization
NAVWAR	Navigation Warfare
NCO	National Coordination Office
NDGPS	Nationwide Differential Global Positioning System

FOR OFFICIAL USE ONLY

NGA	National Geospatial-Intelligence Agency
NII	Networks and Information Integration
NIPRNET	Non-Secure Internet Protocol Routing Network
NIST	National Institute of Standards and Technology
NORAD	North American Aerospace Defense Command
NOTAM	Notice to Airmen
NOTMAR	Notice to Mariner
ns	nanoseconds
NSA	National Security Agency
NSG	National System for Geospatial Intelligence
NSSI	National Security Space Institute
NTP	Network Time Protocol
O&M	Operations and Maintenance
OCS	Operational Control Segment
ORD	Operational Requirements Document
OSD	Office of the Secretary of Defense
OTAD	Over-the-air-distribution
OTAR	Over-the-air-rekey
P-Code	Precise Code (unencrypted)
PNT	positioning, navigation, and timing
POM	Program Objective Memorandum
PPBS	Program Planning Budgeting System
PPS	Precise Positioning Service (GPS)
PPS-SM	Precise Positioning Service-Security Module
PTAN	Precise Terrain-Aided Navigation
PTTI	Precise Time and Time Interval
PVT	Position, Velocity, and Timing
P(Y)	Precise Code (encrypted or unencrypted)
R&D	Research and Development
RCVw	Red Crypto Variable Weekly
RDF	Radio Direction Finder
RGUV	Red GPS Unique Variable
RITA	Research and Innovative Technology Administration
ROMO	Range of Military Options
S&T	Science and Technology
SA	Selective Availability (GPS)
SA/A-S	Selective Availability/Anti-Spoof
SAASM	Selective Availability/Anti-Spoof Module
SAE	Service Acquisition Executive
SARPS	Standards and Recommended Practices
SATCOM	Satellite Communications

FOR OFFICIAL USE ONLY

SCATANA	Security Control of Air Traffic and Navigation Aids
SCAT	Security Control of Air Traffic
SES	Senior Executive Service (U.S. Government)
SIPRNET	Secret Internet Protocol Router Network
SIS	Signal in Space
SMC	Space and Missile Systems Center
SME	Subject Matter Expert/Expertise
SPD	System Program Director
SPS	Standard Positioning Service (GPS)
SV	Space Vehicle
TACAN	Tactical Air Navigation
TAI	International Atomic Time
TNC	Theater NAVWAR Center
TRL	Technology Readiness Level
TSA	Transportation Security Administration
TTP	Tactics, Training and Procedures
TWSTT	Two-Way Satellite Time Transfer
UCP	Unified Command Plan
UE	User Equipment
U.S.	United States
USA	U.S. Army
USAF	U.S. Air Force
USCG	U.S. Coast Guard
USD(AT&L)	Under Secretary of Defense (Acquisition, Technology & Logistics)
USG	U.S. Government
USMC	U.S. Marine Corps
USN	U.S. Navy
USNO	U.S. Naval Observatory
USNORTHCOM	U.S. Northern Command
USSTRATCOM	U.S. Strategic Command
UT1	Universal Time determined from the Earth's rotation
UTC	Coordinated Universal Time
VLF	Very Low Frequency
WAAS	Wide Area Augmentation System (GPS)
WG	Working Group
WGS 84	World Geodetic System 1984
Y-code	Precise Code (encrypted)

FOR OFFICIAL USE ONLY

(INTENTIONALLY BLANK)

FOR OFFICIAL USE ONLY