STRATEGY
for the
DEPARTMENT OF DEFENSE
POSITIONING, NAVIGATION AND TIMING (PNT)
ENTERPRISE
[UNCLASSIFED VERSION]

Ensuring a U.S. Military PNT Advantage

NOVEMBER 2018

DoD Chief Information Officer
Principal Staff Assistant for PNT Policy

This Page Intentionally Left Blank

Table of Contents

This Page Intentionally Left Blank

FOREWORD

The National Security Strategy and National Defense Strategy issued by President Donald Trump and Secretary of Defense James Mattis, respectively, place significant emphasis on the ability of U.S. military forces to operate with lethal effect and to remain resilient in the face of increasing threats from our adversaries around the world. Capabilities provided by the DoD Positioning, Navigation, and Timing (PNT) Enterprise are integral to enabling the Joint Force to achieve those objectives. This Strategy for the DoD PNT Enterprise also serves as an essential element of the Department's Command, Control, and Communications Strategy, which in turn is a component of the even larger DoD Information Technology Strategy.

The challenge of remaining resilient in a dynamic threat environment is compounded by the need to implement new PNT capabilities both rapidly and affordably in many different DoD weapon system applications. This Strategy takes account of the operational and economic realities in play and directs coordinated, coherent actions by all DoD Components with oversight and guidance provided by a DoD PNT Enterprise Oversight Council structure. It leverages the cornerstone capabilities provided by a modernized Global Positioning System with diverse additional sources of PNT information in a modular, open-system integration approach to deliver resilient PNT effects for the Joint Force.

These actions across the DoD PNT Enterprise are necessary to meet both National and DoD Military Strategy objectives. The strategic guidance herein focuses efforts to realize those objectives now and into the future. The DoD is committed to maintaining and reinforcing a military PNT advantage for U.S. and allied forces in all warfighting domains.

This version of the PNT Enterprise Strategy is UNCLASSIFIED to enable its distribution to a broad audience within the U.S. Government and externally. Classified versions at SECRET (NOFORN) and TOP SECRET (SCI) levels are available to properly cleared personnel with Need-To-Know authorization. Contact the office of the DoD Chief Information Officer for further information.

This Page Intentionally Left Blank

INTRODUCTION

State and non-state actors place the safety of the American people and the Nation's economic vitality at risk by exploiting vulnerabilities across the land, air, maritime, space, and cyberspace domains. Adversaries constantly evolve their methods to threaten the United States and our citizens. We must be agile and adaptable.

National Security Strategy, 2017

The U.S. military continues to lead the world in the development and employment of positioning, navigation, and timing (PNT) capabilities, building upon the strengths of the Global Positioning System (GPS), combined with other sources of accurate PNT information to increase resilience and accuracy.

To advance and support U.S. national security and military strategy now and into the future, the DoD civilian and military leadership must remain attuned to the vital enabling role that military PNT capabilities play in shaping the global environment, deterring aggression, fighting and winning today's wars, and in preparing for future challenges.

The U.S. military and its allies are increasingly challenged by threats to our national security and to our PNT capabilities. The DoD must maintain a U.S. military PNT advantage across the continuum of conflict and the range of military operations.

This document presents a strategy for the DoD to provide and assure a PNT Enterprise to the United States Joint Military Force and its allies and coalition partners, ensuring that PNT services and capabilities are available to enable the full range of modern warfare.

This strategy also enables execution of the full range of Navigation Warfare (NAVWAR) Operations by Combatant Commanders to maintain a U.S. military PNT advantage in support of both national security and strategic military objectives.

The PNT Enterprise encompasses governance, capabilities, applications, and effects. It includes the sources of PNT information (global, regional, and

local/natural and manmade), the means of distributing and regulating PNT information, the applications and implementations that exploit various combinations of PNT information, and the effects generated by the use of PNT information in the execution of NAVWAR Operations.

STRATEGIC CONTEXT

The Joint Force must remain capable of deterring and defeating the full range of threats to the United States. The Department of Defense must develop new operational concepts and capabilities to win without assured dominance in air, maritime, land, space, and cyberspace domains, including against those operating below the level of conventional military conflict.

National Security Strategy, 2017

The National Security and National Defense Strategies rely on a well-equipped, capable, and resilient Joint Force to defend and advance U.S. national interests around the world. Elements of PNT are embedded in and are essential to the execution of all Joint Force missions.

Military PNT capabilities developed and acquired by the Services must provide a PNT information advantage to the warfighter in the execution of NAVWAR Operations across the continuum of conflict and the range of military operations in any contested environment.

> This increasingly complex security environment is defined by rapid technological change, challenges from adversaries in every operating domain, and the impact on current readiness from the longest continuous stretch of armed conflict in our Nation's history. In this environment, there can be no complacency—we must make difficult choices and prioritize what is most important to field a lethal, resilient, and rapidly adapting Joint Force. America's military has no preordained right to victory on the battlefield.
>
> General James Mattis,
> Secretary of Defense

These PNT capabilities must be scalable by weapon system and by operational mission requirements and then integrated across the DoD to enable the Joint Force to execute its assigned missions.

The 2018 National Defense Strategy defines a strategic approach which incorporates three specific lines of effort:

1. Build a more lethal force
2. Strengthen alliances and attract new partners
3. Reform the Department for greater performance and affordability.

PNT Enabling National Defense Strategy Objectives

The DoD PNT Enterprise is integral to and plays a key enabling role in executing all three lines of effort defined in the National Defense Strategy. Elements of the PNT Enterprise are embedded in all DoD systems and missions and are essential to their successful operation and accomplishment, respectively.

Build a More Lethal Force

Incorporation of precise PNT information improves command and control coordination, increases communications fidelity and integrity, and increases the accuracy and efficiency of weapon systems at every point in the kill chain, all of which work together to increase the lethality of DoD military operations.

Assured PNT information is the linchpin to ensuring the Joint Force is able to hold the adversary at a disadvantage and to prosecute warfare against the adversary at a time and place of our choosing. Ensuring resilient and trusted sources of PNT information to warfighting systems and fielded forces is critical to meeting all Joint Force requirements for maneuvering in featureless terrain, conducting coordinated cross-domain effort, relying on dispersed ISR sources, coordinating command and control activities via distributed means, and achieving unity of effort with our allies and coalition partners in all-weather day-night operations.

Strengthen Alliances and Attract New Partners

GPS-enabled PNT has been a key element enhancing NATO Alliance interoperability since an initial NATO Team was integrated into the GPS Joint Program Office in the 1970s, and the Memorandum of Understanding (NATO MOU IV) for access to GPS military capabilities has been adopted by all NATO Member States as Alliance membership has grown.

There are also bilateral arrangements with many other U.S. allies and partners regarding access to GPS-enabled PNT capabilities as well as cooperative development agreements, under the authority and oversight of the DoD CIO, for PNT-related initiatives between the DoD and various foreign partners.

Because of its effectiveness in enhancing military operations of all types, GPS-enabled PNT is a significant inducement for cooperation with the U.S. by foreign partners. GPS security is managed under a process defined in DoD compliance issuances, which is designed to deliver PNT capability to U.S. and allied warfighters while maintaining program security.

Currently, 57 countries are authorized access to GPS-enabled military PNT capability. The DoD CIO is the release authority for such access, which is granted through a DoD CIO memorandum. Releases not covered under NATO MOU IV require Combatant Command determination of an interoperability requirement with the foreign nation to support the Joint Force or a specific determination of a political/military requirement by senior DoD leadership.

A list of countries authorized access to GPS military capabilities will be maintained on the DoD CIO website.

Finally, the civil capabilities from GPS, also provided by the DoD, support U.S. and international civil, commercial, and scientific activities around the world. These capabilities produce efficiencies and create benefits which provide tangible demonstrations of the civil and commercial value of GPS to the world. These in turn strengthen U.S. relationships with many nations beyond those with which the U.S. engages in military cooperation and security assistance.

Reform the Department for Greater Performance and Affordability

Elements of the PNT Enterprise contribute to virtually all aspects of business operations, not only for commercial industry but also for the DoD. Improvements to the fidelity of PNT capabilities increases the efficiency and effectiveness of business operations through increased communications throughput, refined production and logistics management, and general command and control of business operations.

Specifically for the DoD, use of accurate PNT enables increased safety and effectiveness of logistics operations which require rendezvous, time-sensitive delivery, or other types of coordination, resulting in decreased operational costs.

Improvements in target location determination, situation awareness, and weapons delivery accuracy also enable safer and more efficient execution of combat operations, resulting in decreased costs in terms of collateral damage in both lives and materiel.

PNT Foundational Role

The advent of GPS created an awareness of the value of an ability to globally know and manage position and time simultaneously and with precision for a variety of purposes. Timing signals from GPS enable precise and dynamic positioning and movement (navigation). Therefore, GPS-derived PNT became the catalyst for dramatic efficiency and safety improvements in military operations.

Consequently, the Joint Force has come to plan, procure, train, and fight with a foundation of continuously available and accurate PNT as a given. Continuous access to GPS signals enhances real-time battlespace awareness for command and control, synchronizes communications, and enables all forms of precision operations from target location to weapon delivery to logistical support.

At the same time, it is increasingly clear that space-based PNT services provided by GPS will be targeted and will not always be available in contested military operating areas, or perhaps globally. Alternative sources of sufficiently accurate PNT information are required to assure continuity of PNT availability as the Joint Force confronts future challenges.

The addition of precise positioning and timing information to the existing foundations of communications and computer technology profoundly changed military command and control from a historically reactive process to a state of near coincidence.

Information latency previously hindered situation awareness and constrained command and control, adversely affecting decision-making. With the advent of continuous global access to precise position and time, advances in information content and currency throughout the battlespace virtually eliminate information latency.

Readily available high precision position and time information gives operational commanders near real-time situation awareness, providing a level of control virtually coincident with battlefield conditions as they develop; from continuous monitoring of blue forces within the battlespace, to prosecuting mobile perishable targets within a time critical kill-chain.

The U.S. military has gained phenomenal force enhancement benefits through the use of GPS-provided PNT services, and the DoD now must take the steps necessary to maintain this PNT advantage into a future where reliance on precise PNT continues to increase while threats to PNT information sources proliferate.

Figure 1 provides a notional representation of the foundational role the DoD PNT Enterprise plays in today's cyber-intensive electronic battlespace. The Cyber Era, enabled in the mid-1990s by precise PNT from a newly operational GPS, affords the Joint Force tremendous warfighting capability through the ability to exercise command and control informed by near real time situation awareness.

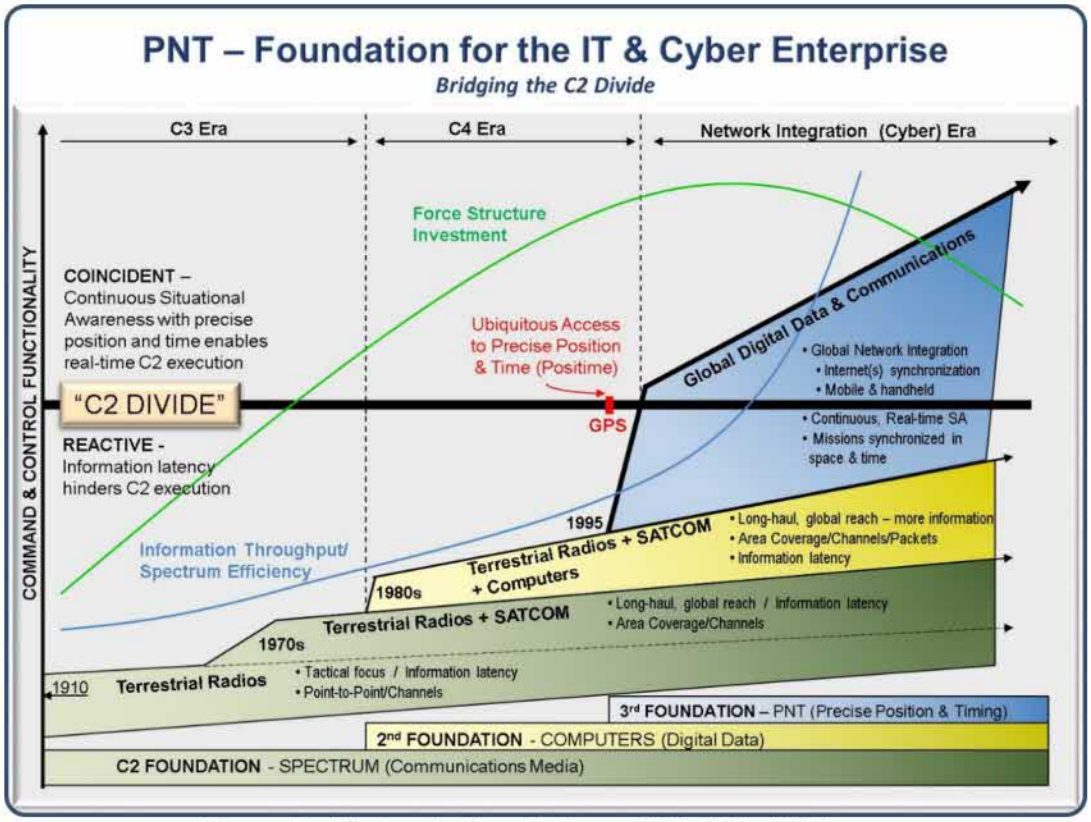

Figure 1 – Electronic Foundations of Joint Warfighting:

1) Spectrum - communications media, (Green)

2) Computers - digital data, (Yellow)

3) PNT - precise position and timing, (Blue)

In the face of these evolving threats and vulnerabilities, it is essential that the entire DoD, from leadership to forces in the field, gain an appreciation for the role of the DoD PNT Enterprise and adopt a holistic view towards its implementation and employment. While GPS will remain the cornerstone PNT capability for the DoD, complementary PNT capabilities must be applied as well using a modular open-system approach to ensure timeliness and affordability in implementation and resiliency in effects. This Strategy defines the means by which the DoD will govern and employ the DoD PNT Enterprise to achieve PNT Dominance for the Joint Force.

POLICY PILLARS OF THE PNT ENTERPRISE

Challenges to the U.S. military advantage represent another shift in the global security environment. For decades the United States has enjoyed uncontested or dominant superiority in every operating domain. We could generally deploy our forces when we wanted, assemble them where we wanted, and operate how we wanted. Today, every domain is contested—air, land, sea, space, and cyberspace.

National Defense Strategy, 2018

In its implementation of the DoD PNT Enterprise for the Joint Force, it is the policy of the DoD that the Enterprise serves three principal functions for the United States:

a. Provides and protects the effective use of military GPS and other PNT services by U.S. and Allied forces anywhere in the world.

b. Prevents the effective use of PNT services by adversaries in areas of military operations.

c. Preserves civil GPS PNT services to non-combatants outside areas of military operations.

Protect U.S. Military Use of PNT Services

PNT information is essential to the execution and command and control of military missions and to the efficient operation of information networks necessary for continuous situation awareness by Combatant Commanders and other senior decision makers.

Protected PNT capabilities enable U.S. and allied forces to effectively employ diverse NAVWAR capabilities to ensure a PNT advantage in support of military operations.

This strategy establishes the DoD way ahead to secure Joint Force military advantages enabled through the exploitation of DoD PNT Enterprise capabilities.

Prevent Adversary Use of PNT Services

In the context of these policy tenets, PNT information contributes extensively to each phase of war, to all joint warfighting functions, and to each joint capability area that enables cross-domain synergy (Figure 2).

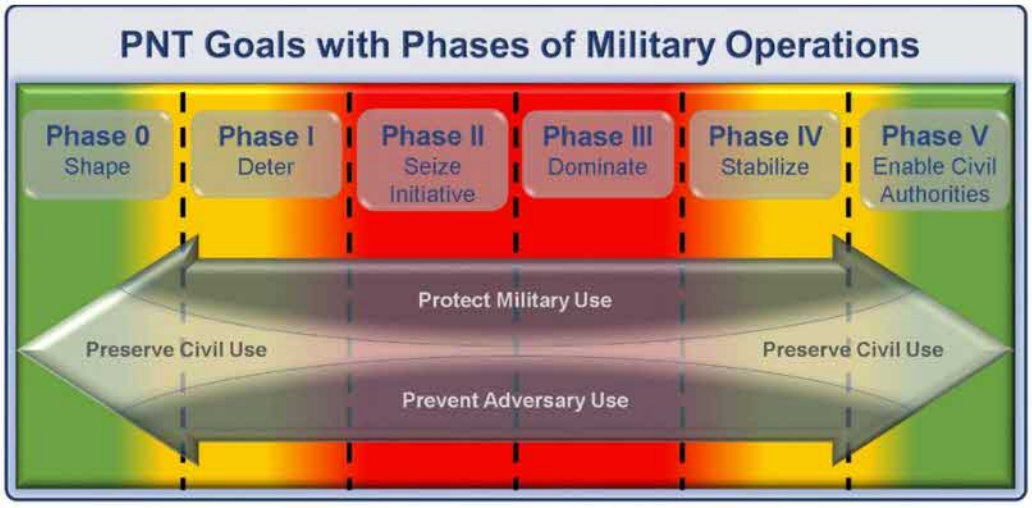

Figure 2 – PNT and **the Phases of Military Operations**

Potential adversaries are becoming more sophisticated in their use of PNT and, in some cases, developing their own PNT systems while simultaneously reducing reliance on GPS. Also, PNT improvements are increasing in lethality. To maintain a PNT advantage, Joint Force Commanders (JFCs) and Combatant Commanders (CCDRs) must be able to execute defensive and offensive NAVWAR operations, ensuring warfighters have access to PNT information when, where, and how they need it and also possess the ability to deny its benefits to adversaries as necessary.

Preserve Civil/Commercial Use of PNT Services

At the same time, recognizing the global value of GPS-provided PNT to civil economic and scientific activities, commanders should make every effort to restrict NAVWAR collateral effects to areas of military operation and limit harmful effects on peaceful civil and commercial uses elsewhere.

Therefore, it is the policy of the DoD to Provide and Preserve, to the maximum extent practicable, civil GPS PNT services to non-combatants outside the area of military operations.

This Page Intentionally Left Blank

THE DOD PNT ENTERPRISE

Failure to meet our defense objectives will result in decreasing U.S. global influence, eroding cohesion among allies and partners, and reduced access to markets that will contribute to a decline in our prosperity and standard of living. Without sustained and predictable investment to restore readiness and modernize our military to make it fit for our time, we will rapidly lose our military advantage, resulting in a Joint Force that has legacy systems irrelevant to the defense of our people.

National Defense Strategy, 2018

This strategy describes the means by which the DoD will employ the DoD PNT Enterprise to achieve and maintain a military PNT advantage for U.S. and allied forces in the presence of challenging NAVWAR environments.

While this strategy features compatibility with commercial and foreign nation PNT information sources, its focus is on supporting DoD NAVWAR objectives.

> We are spoiled because space was a benign environment and GPS was always there, so we just assumed it was always going to be there. We can't assume that anymore. We have to train for a GPS denied environment and we have to build resilient systems to make sure we have the capability to fight in any conditions.
>
> General John Hyten,
> Commander, USSTRATCOM

This strategy also includes the PNT information content and management processes for designing, building, acquiring, managing, operating, and defending the architecture. It entails a diverse infrastructure of space and terrestrial, RF and net-centric, and primary and secondary approaches to all-condition PNT information generation, distribution, protected access, and usage.

As shown in Figure 3, The PNT Enterprise encompasses governance, capabilities, applications, and effects. It includes the sources of PNT information (global, regional, or local; whether natural or manmade), the means of distributing and regulating PNT information, the applications and implementations that exploit various combinations of PNT information, and the effects associated with DoD leadership in PNT Enterprise implementation as well as those directly generated by the use of PNT information in the execution of NAVWAR Operations.

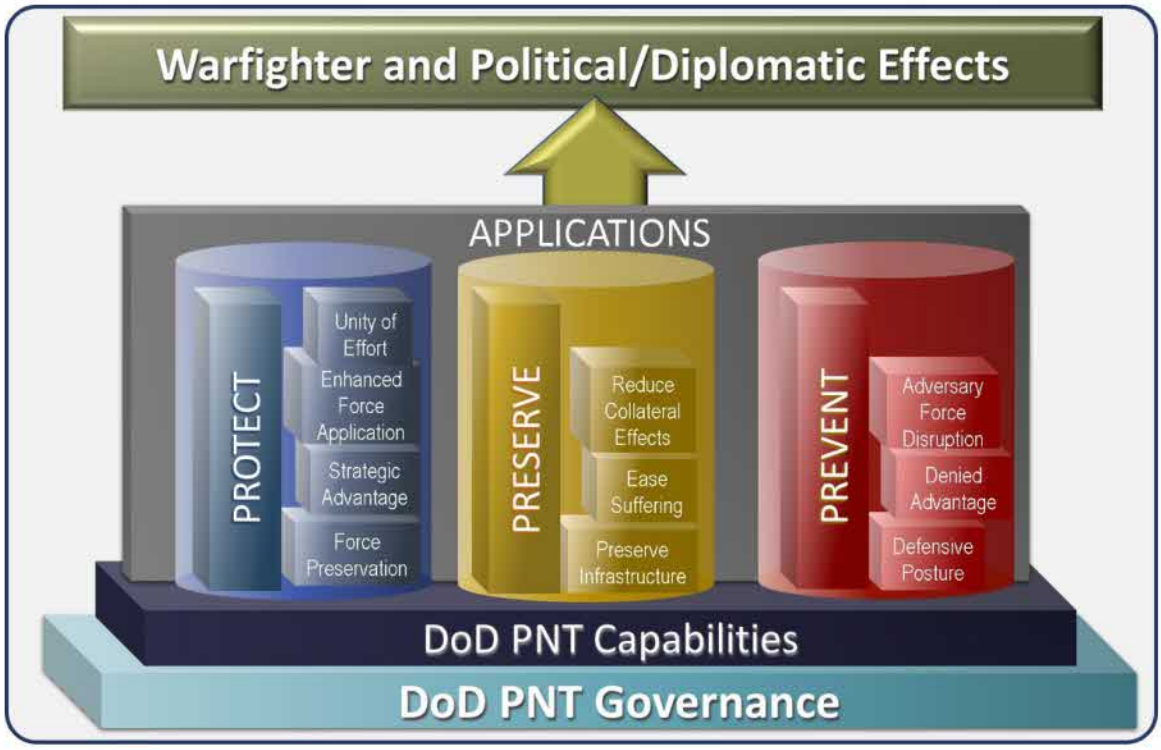

Figure 3 - Functions of the DoD PNT Enterprise

DoD PNT Governance

In executing this strategy, the DoD is guided by statute and presidential policy. Additionally, DoD PNT policies in the DoD Directive (DoDD) 4650.05 family of issuances, under Office of the Secretary of Defense (OSD) authority, establish a compliance framework for the DoD PNT Enterprise. This family of DoD Directives, Instructions, and Manuals provides a coherent and consistent set of PNT policy standards for the DoD.

As a Principal Staff Assistant (PSA) for the Secretary of Defense with responsibility for PNT, the DoD CIO is assigned policy oversight authority for DoD PNT Enterprise capabilities, their application to the Department's military missions, and interagency and international PNT matters affecting DoD interests.

DoD Family of PNT Issuances

In addition to defining the governance structure for the DoD PNT Enterprise, the DoDD 4650 family of issuances address the development and integration of DoD PNT capabilities, the verification of their NAVWAR compliance, and the steps necessary to ensure effective execution of NAVWAR Operations by the Joint Force across the spectrum of conflict.

PNT Oversight Council Structure

As defined in DoDD 4650.05, the DoD CIO chairs a DoD PNT Executive Management Board (EMB) and provides the Secretariat for a senior, congressionally mandated DoD PNT Enterprise Oversight Council (OC). The DoD PNT OC is co-chaired by the Undersecretary of Defense (Acquisition & Sustainment) and the Vice Chairman of the Joint Chiefs of Staff (Figure 4). With support from the EMB and several Working Groups, the OC addresses diverse PNT issues affecting both internal and external Departmental equities and serves as the principal decision body for the DoD PNT Enterprise.

The DoD PNT OC and EMB exercise oversight of DoD PNT Enterprise capabilities, their application to military missions, and interagency and international matters affecting DoD PNT interests.

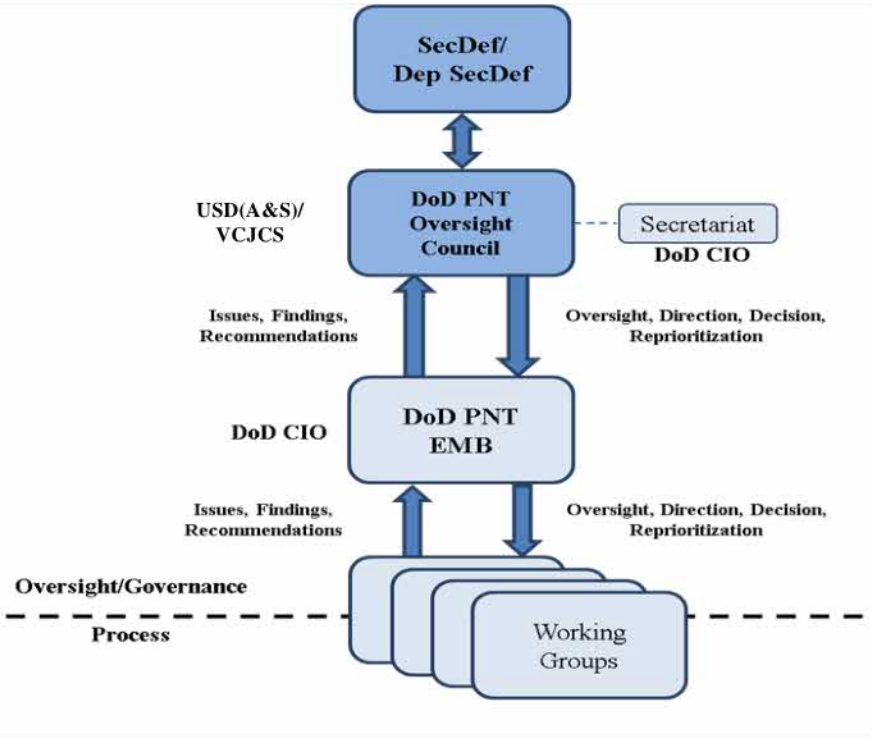

Figure 4 – DoD PNT Enterprise Governance

Roles and Responsibilities

As the Secretary's PSA for PNT Policy and Secretariat for the OC, DoD CIO authorities and responsibilities include determining Department positions and, as necessary, recommendations for OC action on all PNT Enterprise matters affecting DoD interests. This includes matters involving other Federal Agencies and international participants in PNT activities. In developing DoD positions on PNT Enterprise matters, the DoD CIO leads coordination among OC and EMB members.

The DoD CIO establishes and maintains a policy framework for the DoD PNT Enterprise and assigns responsibilities for action and coordination by other DoD Components using the DoDD 4650 family of DoD issuances to ensure compliance. Figure 5 shows the intersection of DoD CIO authorities with those of other principal OC and EMB members who will collaborate and coordinate with the DoD CIO in developing and implementing PNT Enterprise policy initiatives.

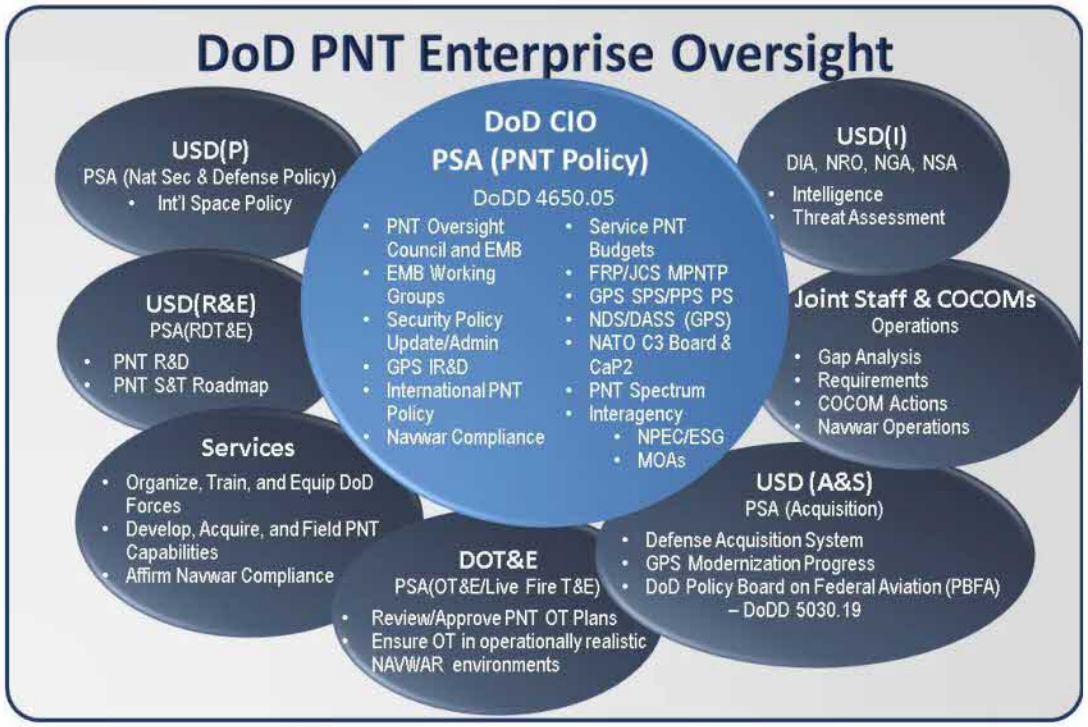

Figure 5 – DoD PNT Enterprise Authorities

a. The Military Services must reflect PNT capability requirements in all system Capability Development Documents and integrate PNT capabilities using an open-system approach as much as possible. Further, Services will develop, acquire, and test integrated PNT capabilities in each system to confirm the ability of the system to meet system survivability requirements for the NAVWAR environments the system will encounter. Both the Undersecretary of Defense for Acquisition & Sustainment USD(A&S) and Service acquisition executives, when acting as Milestone Decision Authorities, must determine and ensure NAVWAR compliance at each acquisition milestone for all platforms and systems using PNT information.

- It is essential that the Services take steps as soon as possible to improve training on proper use of MGUE. This includes implementation of Resiliency and Software Assurance Measures (RSAM) in legacy GPS equipment as well as planning to incorporate M-Code capable GPS receivers at the

earliest opportunity in all Service platforms for which NAVWAR compliance will require M-Code capability.

- Over the longer term, as additional PNT capabilities become available through PNT technology initiatives and are integrated with GPS in a modular open-system approach, it will become possible to achieve NAVWAR compliance through flexible, system- and mission-specific combinations of PNT applications.

b. To ensure broadest application of these requirements, the USD(A&S) will incorporate DoD CIO guidance for PNT and NAVWAR into acquisition and sustainment programs for DoD systems that produce or use PNT information. Specifically, in coordination with the DoD CIO, the USD(A&S) will update DoDI 5000.02, and other supporting guidance as appropriate, to incorporate requirements for MDA determination of NAVWAR compliance at all system acquisition milestones and for major upgrades to fielded systems. This includes the requirement levied by the Congress that all DoD systems using GPS will incorporate M-Code capable GPS receivers when such receivers are available in suitable form factors.

- Because of the importance of GPS to the DoD PNT Enterprise, it is vital that the DoD leadership remain apprised of the progress of GPS modernization efforts. To maintain the necessary level of awareness, the USD(A&S) will conduct progress reviews with the Air Force as required and report GPS modernization status to the OC.

c. As the Combatant Command (CCMD) responsible for space-based PNT and NAVWAR, USSTRATCOM will coordinate employment of space-based PNT capabilities across the DoD and provide a bi-annual assessment of PNT operational capabilities to the DoD CIO. Further, USSTRATCOM will advocate for space-based PNT and joint NAVWAR capabilities, support CCMD joint training and planning related to NAVWAR Operations, and provide contingency NAVWAR Operations support to other CCMDs.

d. USCYBERCOM will advocate for capabilities in support of Joint Force NAVWAR mission requirements and the security and defense of the Department of Defense Information Network (DODIN). As the CCMD responsible for cyber operations, it will coordinate and synchronize DODIN and Defensive Cyberspace Operations necessary to secure and defend DODIN mission

relevant terrain-cyber that enables PNT operations. Additionally, USCYBERCOM will synchronize NAVWAR offensive cyberspace operations in support of combatant commander objectives.

e. To enable and support PNT Enterprise governance, the USD(I) will provide intelligence support to the OC and EMB on PNT-related matters. Through its subordinate organizations, the USD(I) will conduct threat assessments and provide threat reports and analyses to support understanding the characteristics and vulnerabilities of foreign GNSS and other PNT solutions, operational assessments of vulnerabilities and gaps, and determination of NAVWAR environments for use by the Services in assessing NAVWAR compliance for DoD weapon systems and cyber capabilities.

f. Additionally, the National Geospatial-Intelligence Agency (NGA) will maintain and update geospatial reference frames necessary for execution of PNT-enabled operations by the DoD.

g. To support Service and CCMD responsibilities, the Joint Staff will use the Joint Capabilities Integration and Development System (JCIDS) and Joint Strategic Planning System (JSPS) processes for continuing operational assessment of the DoD PNT Enterprise to determine the most effective points for leadership attention and investment to enable rapid, agile application of new and evolving PNT capabilities by the Joint Force. The assessments will inform decisions regarding DOTMLPF-P changes for improved capabilities to address training and TTPs, incorporation of NAVWAR Operations as part of the Unified Command Plan, increases in on-orbit GPS power, attention to terrestrial and airborne pseudolites and other RF systems, accelerated fielding of more robust Military GPS User Equipment (MGUE), improved GPS antennas, non-RF information sharing environments, autonomous PNT information systems, or other solutions.

- STRATCOM and CYBERCOM will support the Joint Staff in conducting the operational assessment with respect to PNT Enterprise applications for Joint Force operations and DODIN functionality, respectively.

h. DOT&E coordinates with the USD(A&S) and DoD CIO to ensure all DoD systems under DOT&E oversight that use PNT information are tested in an operationally realistic NAVWAR environment. Additionally, DOT&E reviews and approves DoD system operational

test and evaluation plans to ensure they are adequate to assess PNT and NAVWAR effectiveness, suitability, and survivability.

To succeed, this effort requires organizations across the DoD to work together to develop the operational concepts necessary to implement and employ PNT capabilities to achieve integrated, seamless PNT-enabled NAVWAR Operations in support of military missions. These integrating operational concepts will provide the basis for each CCMD to incorporate NAVWAR Operations plans to achieve and maintain PNT Dominance in all aspects of military operations.

An Iterative Governance Process

Governance of the DoD PNT Enterprise is exercised by the responsible DoD authorities in Figure 5 through an iterative process as shown in Figure 6.

Figure 6 – DoD PNT Enterprise Governance Process

Policy guidance and compliance issuances are at the heart of the governance process. DoD directives, instructions, and manuals continually affect but are also affected by the other process elements. While such documents are issued by the Secretary, Deputy Secretary, Chairman of the Joint Chiefs, and DoD CIO, each of those leaders is informed by a governance process conducted through the DoD PNT Enterprise OC structure. The process is iterative, driven by the annual DoD budget cycle, through which PNT threats are

evaluated, gaps are determined, capabilities are developed, and applications are implemented to ensure NAVWAR compliance for all elements of the DoD Joint Force structure and supporting information systems.

The process will start with updated threat analyses, generated through Validated Online Lifecycle Threat (VOLT) Reports for programs of record and augmented by special analyses requested from or generated by the Intelligence Community. Based upon the evolving threat, CCMD OPLANS will be evaluated against the existing PNT Enterprise Architecture to identify gaps and shortfalls which represent vulnerabilities to the Joint Force.

Regular reviews and biennial updates of the DoD PNT Science and Technology (S&T) Roadmap maintained by the USD(R&E) in conjunction with Service RDT&E facilities, together with inputs from DARPA and industry, will identify candidate capabilities to augment the operational PNT Enterprise. Services will employ a collaborative Modeling and Simulation (M&S) environment to evaluate candidate capabilities. These evaluations will in turn inform program Analyses of Alternatives (AoAs) which, using realistic operational scenarios, will identify candidates for installation into Joint Force systems using modular, open-system integration approaches to the maximum extent practicable.

Issue papers for candidate upgrades will be evaluated during the annual Program Review, and funding will be programmed as determined by DoD leadership in the annual DoD President's Budget submission to the Office of Management and Budget (OMB).

Multi-source PNT Capabilities

The GPS Precise Positioning Service (PPS) is the principal source of PNT information for the DoD. However, GPS signals can be affected by various sources of interference and are targeted by adversaries. To combat these man-made and natural threats to GPS, other sources for PNT information are necessary to assure continuous PNT service for military users. The space-based GPS is only one element of a multi-layered DoD PNT Enterprise Architecture comprising many potential sources of PNT information. The DoD's overdependence on GPS has become a vulnerability that must be addressed through the incorporation of alternative and complementary PNT capabilities. The DoD must pursue alternative PNT sources and integrated PNT devices for military use during those operational situations when GPS is unavailable or is unreliable.

GPS as a Cornerstone

GPS remains a cornerstone DoD PNT capability, and must continue to be modernized to meet warfighter needs. DoD must focus on synchronizing the GPS satellites and ground control segments with the development and deployment of improved receiver technology as soon as possible. However, intentional and unintentional electronic emissions interfere with GPS signals at the receiver. Physical obstructions can also prevent consistent GPS reception.

> Today, almost every weapon we drop is a GPS guided weapon. Almost our entire force structure is built on GPS guidance. Our dropping of logistics off aircraft are GPS guided, the timing systems for weapons systems are GPS dependent, artillery and GMLRS are GPS guided, Navy Systems are GPS guided. In the future, we have to look at positioning, navigation, and timing as a mission, and build resilience into that architecture, as well as defending GPS on orbit.
>
> General John Hyten,
> Commander, USSTRATCOM

The GPS is also noteworthy in that it is a dual-use (civil and military) capability provided by the DoD which has been used as a model for other Global Navigation Satellite Systems (GNSS) implemented by foreign nations. In accordance with statute and policy, the strategy adheres to the U.S. Government commitment to also provide a globally available GPS service for peaceful civil, commercial, and scientific use. It must also be recognized in this context that growing civil dependence on GPS services for critical infrastructure and public use will continue to constrain the ability of the DoD to maintain a military PNT advantage from GPS.

GPS is and will remain the primary military PNT service. GPS provides the U.S. and allied/partner military users the simultaneous ability to passively, precisely, and dynamically determine three-dimensional position, velocity, and precise time information anywhere in the world and in space to beyond geosynchronous orbit. GPS modernization initiatives are underway to strengthen GPS resiliency, throughout the DoD, and to increase GPS power from space over the next decade.

Those modernization efforts must continue and be synchronized across the GPS satellite, control and user segments for operational implementation as soon as possible. However, GPS vulnerability to threats from relatively low-powered noise jammers and from more sophisticated "smart" jammers or spoofers has long been acknowledged and must be addressed as GPS modernization proceeds. Consequently, to combat man-made and natural

threats to GPS, other sources of PNT information will be necessary to assure continuous PNT service for military users.

Multi-layered PNT Architecture

Integrated, multi-source PNT capabilities will be essential for continuity of situation awareness, information synchronization, and command and control for Joint Force missions. PNT capabilities available to the DoD PNT Enterprise comprise a layered PNT architecture consisting of global, regional, and local sources of PNT information (Figure 7).

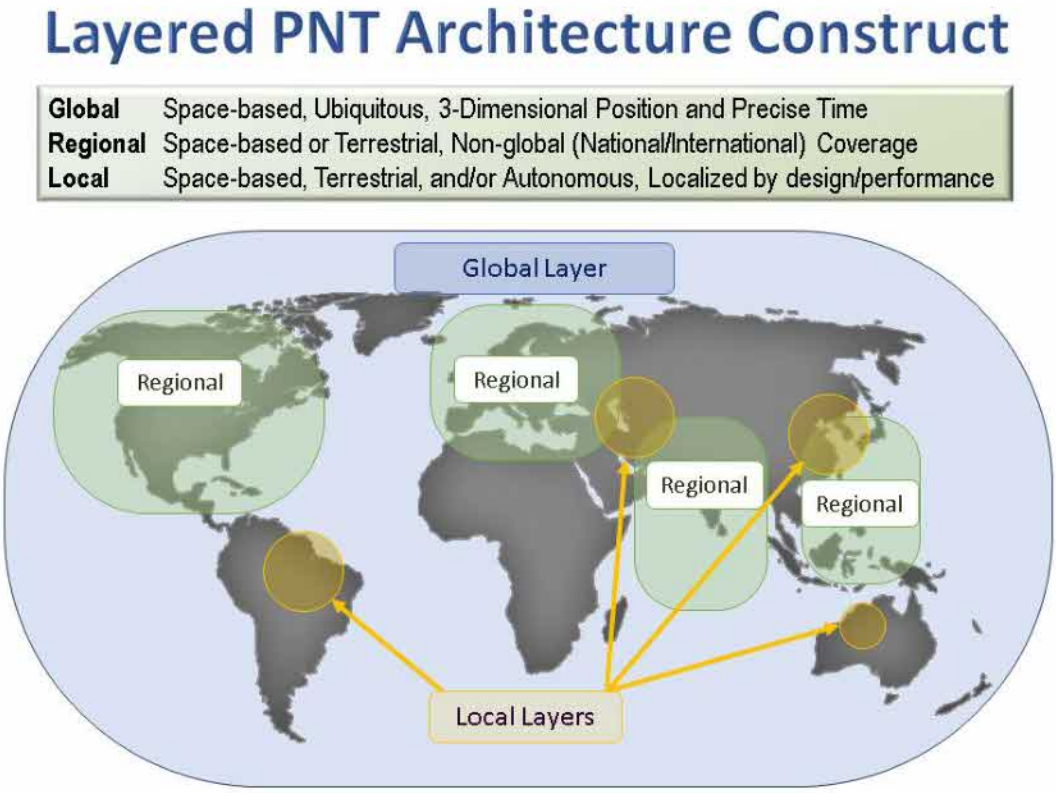

Figure 7 – Layered PNT Enterprise Architecture

The global PNT layer is space-based and available worldwide. The regional PNT layer may be implemented in areas of particular national interest around the world where PNT resiliency must be assured with backup capability. The local layer provides PNT information using manmade and

natural information sources available for a limited time or over a limited area when global or regional PNT information may not be available.

When integrated, tested, and verified for NAVWAR compliance by system providers, operation of the integrated system must be seamless as much as possible based upon system and mission. The employment of multiple PNT sources should not require user awareness or intervention to switch among alternatives during mission execution unless the user elects that option. This approach will enable access to diverse PNT information sources in a way that enables complete mission accomplishment even if one or more of the PNT sources becomes unavailable or unreliable during the course of a mission.

Global PNT Layer

Services from the GPS military PPS comprise the predominant global source of PNT information for the Joint Force. GPS PPS signals are available to the U.S. and allied military and other authorized users at multiple frequencies on a continuous global basis, enabling very precise determination of three-dimensional position and time. Military PPS receivers are designed to operate in the presence of jamming and spoofing through the application of advanced signal processing, encryption, and anti-spoof techniques. Still, the GPS signals are relatively weak in comparison to possible jamming sources, and they cannot always be received in physically obscured environments. DoD policy permits the use of services from other GNSS providers for certain missions to improve availability and resiliency, consistent with NAVWAR compliance requirements. However, the DoD has not conducted the thorough engineering and information assurance assessments necessary to determine whether these systems can assure the Joint Force the degree of PNT integrity available from GPS, and all are vulnerable to the same interference and jamming effects that could jeopardize GPS PPS reception. Consequently, other sources of PNT information with different characteristics are necessary.

Regional PNT Layer

Regional sources of PNT information are those which are available over large areas, but are not global. They may be space-based or ground-based and may cover a few countries or even a continent. Space-based communications systems, with global connectivity that incorporates GPS content, could be used as sources of PNT information for both regional and local areas depending on the number/coverage of leased communications downlinks employed.

Examples of ground-based regional systems include, among others, low-frequency systems such as Enhanced Loran (eLoran) and Spatial, Temporal, and Orientation Information in Contested Environments (STOIC) technologies. Through analyses and demonstration, both systems have been assessed as potential complements to GPS as part of a resilient integrated PNT architecture. Their high power and low frequency enable regional/nationwide coverage, spectrally separate from GPS services, accessible in buildings and under water, and transmitted from dispersed terrestrial locations. Each can be considered as a possible complement to GPS depending on operational circumstances and requirements.

Local PNT Layer

Localized PNT sources are those which are available over a limited geographical area or are available at mission-essential levels of precision for a limited time because of drift rates which require recalibration. They include local area ground-based radiofrequency PNT services, hybrid PNT services integrated with communications systems and data networks, and autonomous PNT sources which operate without external input once calibrated or which sense the local environment automatically. These last devices may operate using stored databases of physical features or they may operate based on real-time sensory inputs.

Integrated PNT Applications for the Joint Force

It is not necessary that the entire Joint Force be equipped with all available PNT capabilities, as that would be cost prohibitive as well as technically infeasible for many platform types. For effective PNT employment, however, forces must be equipped with PNT capabilities based upon system requirements and operational mission profiles that enable compliance for survivability in expected NAVWAR environments.

The DoD is moving rapidly to accelerate availability of resilient PNT for the Joint Force. This is being accomplished through leveraging parallel DoD S&T efforts to implement multi-source PNT capabilities in DoD systems using PNT modular open-system approaches and to increase collaboration in PNT Modeling and Simulation (M&S) and virtual integration techniques. Implementing these initiatives will enable the Joint Force to match and outpace the evolving threat in a broad range of operating environments across the warfighting domains.

Modular Open-System Approach

A multi-source PNT open architecture will enable and promote timeliness and affordability while enabling each service to "tailor" PNT capability combinations in applications appropriate to each platform and mission.

Figure 8 shows a layered range of possible PNT sources on the left, each with the potential of connecting to a Service PNT fusion device (the Integrated PNT Engine) through a standard interface (based upon open-architecture frameworks) and thus providing resilient, NAVWAR compliant PNT capability to support NAVWAR Operations by the Joint Force. The graphic also shows time dissemination from the U.S. Naval Observatory to both the applicable PNT source layers as well as to Defense Regional Clocks at diverse locations. The processes are supported by a collaborative M&S environment and address threats/gaps identified by the operational community. Current initiatives are focused on achieving initial availability of open-system PNT capability applications as early as FY 20/21. This reflects the emphasis placed on bringing modular open-system approaches into operational use as soon as possible to support National Defense Strategy objectives and enable rapid integration of new PNT capabilities with GPS in as many DoD systems as possible. It is important in implementing such approaches that the resilient PNT architecture is also protected from cybersecurity threats, and that new vulnerabilities are not introduced with an increased number of interfaces in a modular open system environment.

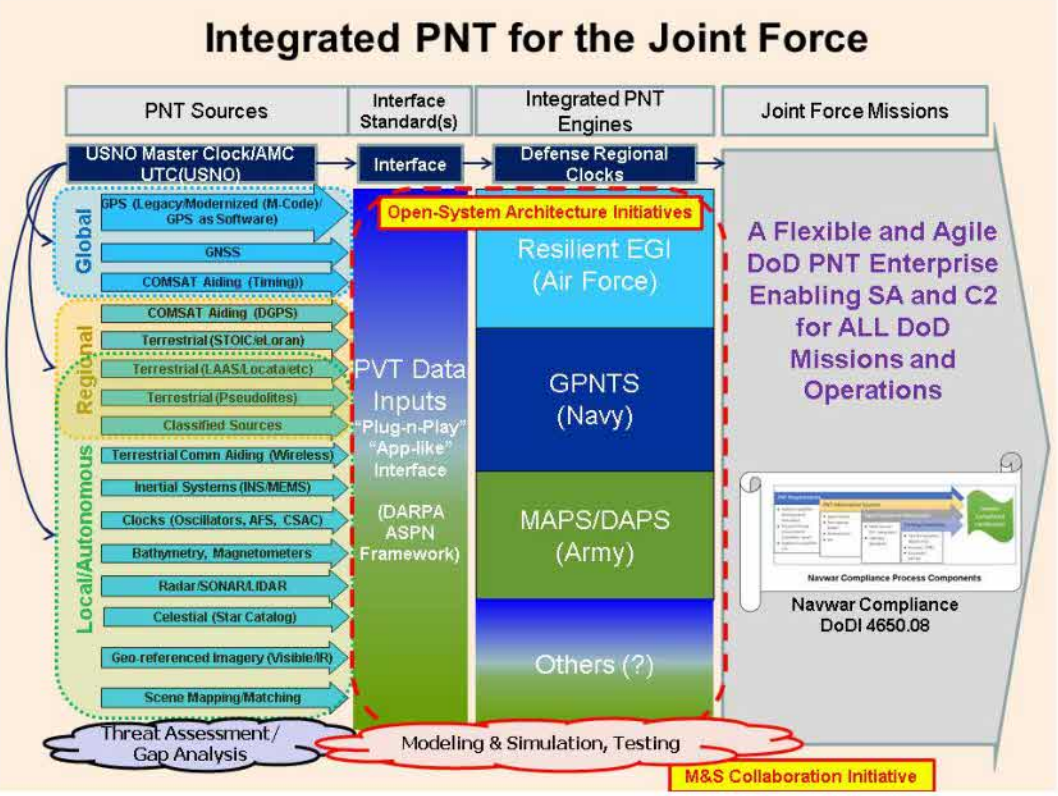

Figure 8 – Notional Capabilities-to-Applications Process

PNT Input/Output Interface Standards

The key to achieving a fully usable and flexible open-system approach to PNT capability integration rests in agreement among the Services on a set of input/output PNT standards to interface with platform data busses and enable multi-source PNT-enabled mission operations as well as platform operations, where necessary. Much effort has been expended on development and demonstration of candidate standards, and it is vital that these efforts be brought into operational service as soon as possible for installation on all DoD platforms during initial weapon system production and retrofit/upgrade activities.

Modular Implementation

The use of modular open-system approaches for future integration of multi-source PNT capabilities will also remove the burden of planning for such integrations from the GPS user equipment program of record. Timely

implementation of GPS modernization capabilities represented by M-Code and other GPS-specific functionalities is essential to increasing resilience of the DoD PNT Enterprise for the Joint Force. The need to consider the addition of other non-GPS PNT sources in GPS program of record receiver designs has been a distraction which has contributed to delays in availability of multi-source integrated PNT capabilities for the Joint Force. Henceforth, the combination of other promising, non-GPS sources of PNT information with modernized GPS capabilities will be accomplished separately from the GPS program of record.

To maintain an asymmetric PNT advantage, the Services must prioritize weapon systems and missions to enable systematic and cost effective integration of improved PNT capabilities to address the increasing threat. Prioritization should focus on those weapon systems that CCMDs will employ for highest priority missions in contested environments, along with the supporting infrastructure and networks upon which DoD operations depend.

Additionally, for each weapon system, to preserve the advantage gained from multi-source PNT operation, the unique combination of PNT capabilities employed to achieve NAVWAR compliance must be protected. Therefore, Services must ensure Security Classification Guides for all programs using PNT information protect the specific PNT technologies and integration methods necessary for the program to be certified for NAVWAR compliance.

Organizational Responsibilities

Organizational responsibilities assigned to implement this modular open-system approach are documented in detail in the DoDD 4650 family of issuances. In summary:

a. The Joint Staff will oversee the documentation of PNT threat scenarios.

b. The Joint Staff will coordinate with other CCMDs on any NAVWAR Operations requirements proposed by STRATCOM.

c. The Military Services will ensure weapon system survivability requirements and system test plans reflect realistic NAVWAR environments for supported missions to enable determinations of NAVWAR compliance by MDAs. The Services will employ modular open-system approaches to achieve NAVWAR compliance, field resilient PNT capabilities in applications meeting mission requirements, and provide flexibility for meeting future challenges.

d. The USD(R&E) will oversee the development of PNT capabilities in the DoD PNT S&T Roadmap and the implementation of PNT open-system integration approaches by the Services to incorporate multi-source PNT capabilities in DoD systems and platforms.

e. The USD(A&S) will incorporate appropriate guidance in Defense Acquisition System issuances to fully implement a NAVWAR compliance verification process by Service acquisition and test organizations.

f. USSTRATCOM and USCYBERCOM will advocate for PNT-enabled joint NAVWAR capabilities and ensure necessary actions are taken to ensure DoD operations are not impacted by hostile or malicious attacks against DoD PNT assets.

g. The DoD PNT Enterprise EMB and OC will oversee the implementation of this DoD PNT Enterprise strategy by all DoD Components.

h. DOT&E will review and approve test and evaluation plans (including cybersecurity test plans) related to the PNT open-system integration approach for systems under DOT&E oversight.

DOD PNT ENTERPRISE EFFECTS

Within the DoD, precise PNT capabilities are fundamental to nearly all joint concepts, including Major Combat Operations, Homeland Security, Battlespace Awareness, Force Application, Global Strike, and Command and Control (C2). Precise PNT is critical to achieving the tenets of the DoD's Future Joint Vision, and is exemplified by use of precision guided munitions (PGMs), handheld battlefield navigation units, and time/frequency-dependent network-centric operations.

National PNT Architecture Study

Effects resulting from the application of PNT capabilities by the DoD include political and diplomatic effects associated with DoD leadership in PNT Enterprise implementation as well as military effects directly generated by using PNT information in the execution of NAVWAR Operations (Figure 9). It is essential in the execution of this strategy that the DoD leadership at all levels be familiar with both these vital areas of influence and that senior leadership be fully engaged in their oversight through the DoD PNT Enterprise OC structure.

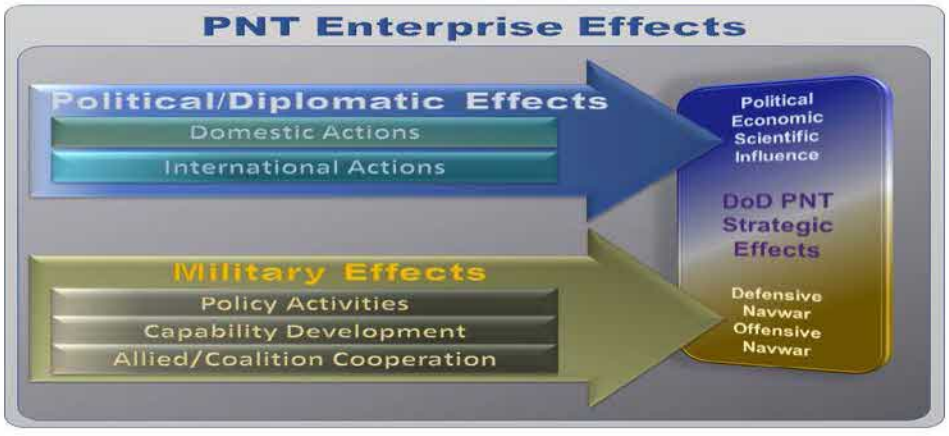

Figure 9 –PNT Enterprise Effects

Political/Diplomatic Strategic Effects

The DoD PNT Enterprise will continue to represent a pervasive technology impact to ever-expanding applications of time and location for commercial, scientific, and military purposes. In the intersections of the Enterprise with domestic and international civil and military interests, the DoD must maintain a constant and authoritative role to preserve the military advantages gained from PNT superiority.

Domestic Strategic Effects

Statute and Presidential policy require that the DoD coordinate with other federal agencies regarding civil use and modernization of GPS for peaceful purposes and facilitate access to appropriate levels of GPS services and user equipment by federal agencies to meet requirements for homeland security purposes.

In executing these responsibilities, the DoD must take steps to ensure the civil agencies are aware of and are sensitive to the dual-use implications inherent in GPS and other PNT Enterprise applications. From this point forward, many of the specific PNT capabilities and combinations of PNT capabilities employed by the DoD for military purposes will increasingly be classified. This is because of the importance of their direct application to force protection for the DoD and its allies and partners and to the execution of warfighting missions by the Joint Force. Such capabilities are not appropriate for use by civil interests, even for such purposes as critical infrastructure protection, because of their potential for compromise and misuse for hostile purposes by unauthorized parties.

Also, even many of the openly available PNT capabilities employed by civil agencies and the public can pose a threat when used improperly or in unauthorized ways by hostile parties. Therefore, caution must be exercised by all parties in advertising and employing such PNT capabilities, whether for domestic purposes or internationally.

The DoD has a statutory responsibility, along with the Departments of Transportation and Homeland Security, defined in United States Code, Title 10, Section 2281 to write and publish a biennial Federal Radionavigation Plan (FRP) to reflect the policy and planning for federally provided common use (i.e., systems used by both civil and military sectors) PNT radionavigation systems.

The DoD will:

a. Continue to cooperate closely with the other federal agencies in preparation and production of the FRP;

b. Continue to coordinate with the other federal agencies regarding operation and modernization of the GPS and support civil-funded modifications to the GPS to meet emerging civil requirements;

c. Continue to support federal agency requests for access to military GPS capabilities as necessary, and complete and maintain required Memoranda of Agreement to validate and document access as authorized;

d. Continue to maintain peacetime coordination with federal agencies regarding military training and exercise requirements, spectrum access and protection, and civil PNT services provided through GPS in accordance with the Standard Positioning Service Performance Standard (SPS PS);

e. Apprise federal agencies of GPS vulnerabilities which may affect civil use of GPS services;

f. Coordinate with and advise federal agencies in civil-funded development and implementation of remediation techniques and technologies to address possible disruption of civil GPS services.

International Strategic Effects

The DoD engages in extensive coordination with international civil and military authorities to both promote the peaceful use of GPS worldwide as well as to maintain a PNT advantage for U.S. and allied militaries. The benefits to the U.S. from exploitation of PNT capabilities range from pursuing mutually beneficial economic and scientific initiatives and peacefully shaping the actions of potential adversaries all the way to conducting precise military engagements.

The ability to maintain an asymmetric advantage from the DoD PNT Enterprise in every environment creates opportunities to expand the U.S. partner and ally base and is both a deterrent to and a target for adversaries.

The DoD will:

a. Continue to participate in U.S. delegations to civil multi-lateral forums such as the International Committee on GNSS and its Providers' Forum and in civil bi-lateral discussions with foreign nations which present opportunities to advance U.S. objectives which benefit the DoD PNT Enterprise.

b. Continue to support the NATO Memorandum of Understanding on GPS and participate in and lead initiatives within NATO for implementation of PNT Enterprise capabilities which benefit NATO Alliance interoperability.

c. Continue to advocate for spectral separation between GPS M-Code and civil/foreign authorized and open services in all international venues.

Military Strategic Effects

Statute and policy require that the DoD maintain and modernize the GPS, as well as develop, implement, and maintain applications to integrate GPS and other PNT capabilities for use in contested environments, while preventing adversaries from employing the same capabilities.

The capabilities inherent in modernized GPS satellites, ground systems, and receivers will enable flexibility for commanders to execute a full range of protect and prevent options. The capabilities of the modernized GPS, with spectrally separate M-Code, will also enable employment of applications which will enhance the ability of commanders to prevent adversarial use of PNT in areas of operation. Timely operational employment of modernized GPS capabilities by the Joint Force is essential and is a priority of the Department.

Foreign militaries and non-state actors recognize the benefits of space-based PNT and the value of GPS to military operations as demonstrated by the U.S. and its allies/partners since GPS was first widely used during Operation Desert Storm. For the Joint Force, continuous access to GPS-quality PNT, as defined in the GPS Precise Positioning Service (PPS) Performance Standard, enables near real-time situation awareness for command and control, synchronizes communications and supports all forms of precision operations from target location and weapon delivery to on-time logistical support.

Foreign governments have followed suit and embraced PNT as a force enhancer. Some have built or are building their own Global Navigation Satellite Systems (GNSS). These include global systems such as the Russian Global Navigation Satellite System (GLONASS), the European Galileo, the Chinese BeiDou, as well as regional systems such as the Japanese Quasi-Zenith Satellite System (QZSS), and India's Navigation with Indian Constellation (NavIC).

Use of foreign GNSS signals is one PNT capability option within the DoD PNT Enterprise. The DoD is prohibited by statute from using non-allied signals in DoD systems. However, with careful analysis and thorough understanding of allied GNSS services, use of such services may be possible in the future as a part of the DoD PNT Enterprise. Under the modular open-system integration approach, additional PNT capabilities may be incorporated into military weapon systems as they are determined to be acceptable for use and as they are necessary to meet system or mission requirements.

In accordance with DoD PNT policy, acquisition decision authorities must ensure future military weapon system PNT capabilities are compliant with

the survivability requirements of the NAVWAR environments in which they must operate. Under this concept, signals from Galileo, QZSS, and other sources may be incorporated as appropriate and required.

Navigation Warfare (NAVWAR)

NAVWAR comprises the effects from combinations of defensive and offensive applications of DoD PNT Enterprise capabilities through coordinated employment of space, cyberspace, and electronic warfare operations affecting all warfighting domains. Characterization of offensive and defensive capabilities in all warfighting domains (Figure 10) is key to defining the NAVWAR environment and leveraging it for warfighting purposes. This includes:

a. Battlespace awareness of adversary dependencies and vulnerabilities;

b. Battlespace awareness of space, cyberspace, and RF threats to Joint PNT Assurance;

c. Kinetic threats to PNT information infrastructure;

d. Real-time status of the RF spectrum and cyberspace;

e. Availability and status of Joint NAVWAR capabilities.

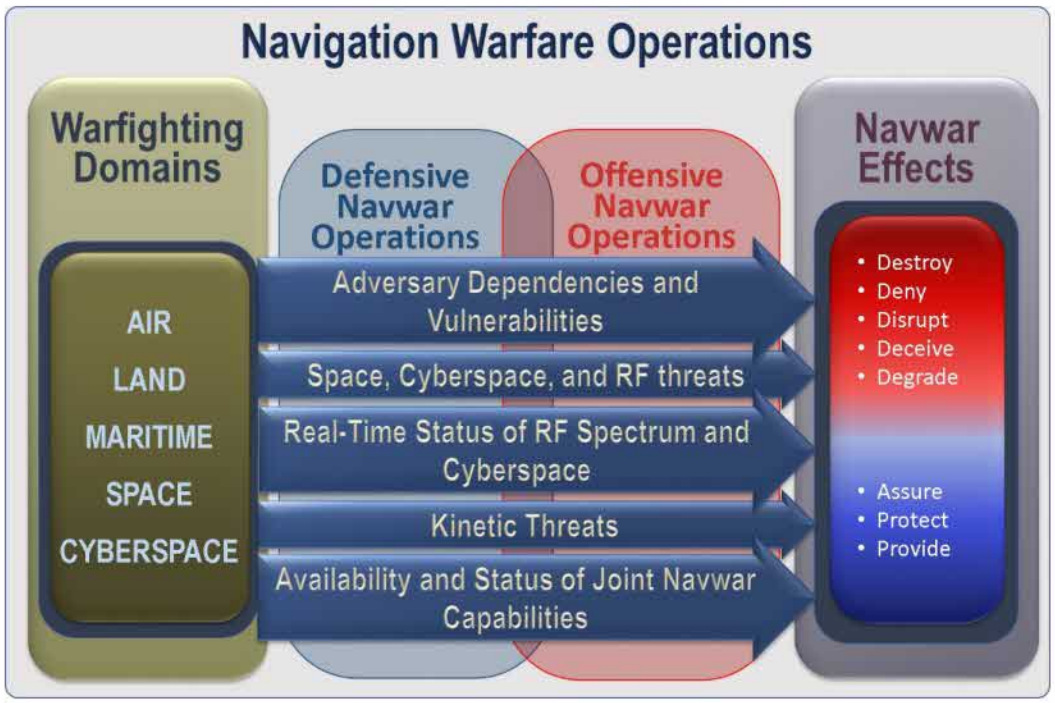

Figure 10 – Navigation Warfare Operations

DoD policy states that U.S. and allied forces must effectively employ NAVWAR to ensure a PNT advantage in support of military operations. This requires all DoD systems to become NAVWAR compliant and that compliance be tested and verified by DoD acquisition and appropriate test authorities.

A system will be determined to be NAVWAR compliant if it continues to provide trusted PNT information over the time period required by a specific mission at the level of accuracy required by the mission in the expected physical, electromagnetic, and cyber environment.

Defensive NAVWAR

The DoD makes use of a layered architecture of PNT capabilities to prevent degradation of NAVWAR Operations due to interference with or other disruption of the PNT information sources employed in DoD systems. The use of diverse sources of PNT information, integrated and validated for compliance with intended NAVWAR environments, ensures continuity in the operation of PNT-enabled applications in DoD weapon systems and platforms.

The DoD will:

a. Employ as much as possible a modular open-system approach to integration of DoD PNT Enterprise capabilities into DoD platforms and weapon systems to enable maximum flexibility and unpredictability in dealing with the evolving NAVWAR threat environment.

b. Conduct discussions and establish agreements with U.S. allies and coalition partners regarding acquisition and employment of PNT Enterprise capabilities to minimize fratricide and ensure interoperability in combined NAVWAR operational environments.

Offensive NAVWAR

NAVWAR counter-PNT options take into account various strategic, operational, and tactical assets. The Joint offensive NAVWAR capability inventory may comprise any asset operating in the physical or cyberspace domains or in the RF spectrum (whether currently associated with the PNT mission or not) which could be called upon to produce kinetic or non-kinetic adverse PNT effects on an adversary.

Warfighters must take into account, in exercising NAVWAR offensive operations, the integrating role PNT plays across the information enterprise, for both friendly and hostile forces. PNT is a fundamental enabler of the enterprise and is necessary for efficient operation of telecommunications and information systems. Such PNT enabled systems are integral to command and control of military forces, effective employment of weapons, and many essential military and intelligence missions. Readily available precise position and time offer near real-time situation awareness for both U.S. and adversary forces. In that context, PNT is a vital element of U.S. and adversary IT architectures.

To further the objective of achieving PNT Dominance, the DoD will:

a. Ensure U.S. and allied/coalition forces use PNT devices incorporating diverse but known and well-characterized sources of PNT information. Effective execution of offensive NAVWAR options requires complete awareness of the range of PNT capabilities and applications in use by U.S. and allied/coalition forces to avoid fratricide.

b. Accelerate Service initiatives to implement modular open-system approaches for PNT capability integration to accelerate availability of applications that enhance flexibility for offensive NAVWAR.

c. Continue to press for rapid fielding of GPS M-Code receivers, which are essential for the U.S. to fully enable electronic attack and exploit the advantages inherent in GPS modernization initiatives.

This Page Intentionally Left Blank

WAY AHEAD

For decades the United States enjoyed uncontested or dominant superiority in every operating domain or realm. We could generally deploy our forces when we wanted, assemble them where we wanted, and operate how we wanted. Today, every operating domain is contested.

General James Mattis, Secretary of Defense

As the President and Secretary of Defense have indicated, the Joint Force must be prepared to confront and defeat aggression anywhere in the world in a dynamic and increasingly challenging environment. The DoD PNT capability lies at the heart of Joint Force global readiness. The United States faces profound challenges that require strong, agile, and capable military forces enabled by integrated PNT capabilities.

Our country is challenged by multiple adversaries with an expanding range of capabilities available to them. To maintain military superiority in this multi-domain world, we must out-think, out-maneuver, out-partner, and out-innovate our adversaries.

General John Hyten,
Commander, USSTRATCOM

As a PSA for the Secretary of Defense, the DoD CIO has oversight authority for PNT policy affecting DoD PNT capability requirements, acquisition, and application to the Department's military missions, as well as interagency and international PNT matters affecting DoD interests. It is important to restate and highlight with respect to these policy responsibilities that the family of DoD Directives, Instructions, and Manuals under DoD Directive 4650.05 provides a coherent and consistent set of PNT policy standards for the DoD.

As Secretariat for the DoD PNT Enterprise OC and as Chair of the DoD PNT EMB, the DoD CIO is the Department focal point for oversight of all PNT Enterprise actions affecting both internal and external Departmental equities. Implementation actions assigned in this strategy document reflect

Component responsibilities included in the DoDD 4650.05 family of issuances. Execution of implementation actions will be tracked through regular meetings of the DoD PNT Enterprise OC and EMB.