United States Government Accountability Office

Report to the Committee on Armed Services, U.S. Senate

August 2022

GPS ALTERNATIVES

DOD Is Developing Navigation Systems But Is Not Measuring Overall Progress

Accessible Version

GAO-22-106010

GAO Highlights

Highlights of GAO-22-106010, a report to the Committee on Armed Services, U.S. Senate

August 2022

GPS ALTERNATIVES

DOD Is Developing Navigation Systems But Is Not Measuring Overall Progress

Why GAO Did This Study

DOD primarily relies on GPS for accurate PNT data, which is essential to effective military operations. However, multiple threats can render GPS data unavailable or inaccurate. DOD recognizes the threats to GPS and is taking steps to address them by developing more robust GPS capabilities and alternative PNT technologies.

GAO was asked to review DOD's acquisition of alternative PNT technologies. This report discusses (1) the threats facing GPS; (2) DOD's alternative PNT efforts and their business cases; and (3) DOD's oversight of its PNT portfolio. This is a public version of a sensitive report that GAO issued in April 2022. Information that DOD deemed to be sensitive has been omitted.

GAO compiled and analyzed GPS threat information from relevant organizations and DOD officials; analyzed DOD documents; reviewed DOD PNT portfolio plans and strategies; interviewed DOD officials; and sent a questionnaire to DOD PNT program officials and analyzed results.

What GAO Recommends

GAO recommends that the Secretary of the Navy ensure the Navy's alternative PNT efforts have complete business case elements, such as an acquisition strategy. GAO also recommends that the PNT Oversight Council establish strategic objectives and metrics to measure the progress of its PNT portfolio overall. DOD concurred with one recommendation and partially concurred with the other. GAO maintains both recommendations are valid.

View GAO-22-106010. For more information, contact Brian Bothwell at (202) 512-6888 or BothwellB@gao.gov, or Jon Ludwigson at (202) 512-4841 or LudwigsonJ@gao.gov.

What GAO Found

The U.S. military relies on its Global Positioning System (GPS) to provide position, navigation, and timing data crucial to its operations. Access to these data, collectively known as PNT, and GPS face multiple threats, including: (1) anti-satellite weapons, (2) jamming, (3) spoofing, and (4) cyber. Given GPS's vulnerabilities, the Department of Defense (DOD) is modernizing GPS by adding a stronger encrypted signal, known as M-code, and using technologies like anti-jam antennas. Even with upgrades, vulnerabilities will remain.

The military services are developing alternative PNT capabilities to complement GPS. Of the five PNT efforts that have started development, four efforts had incomplete business cases (see figure). Specifically, the Navy had incomplete business cases for its four alternative PNT efforts, as the Navy either did not have or was drafting business case elements. A complete business case gives decision makers information at the start of product development to set the program up for success and can limit cost, schedule, and technical problems.

Status of Business Case Documents for Alternative Position, Navigation, and Timing (PNT) Efforts in Development

Effort	Requirements documentation	Acquisition strategy	Assessment of technology risk	Assessment of schedule risk	Independent cost estimate
Navy's Automated Celestial Navigation System	●	●	○	○	●
Navy's PNT upgrade to Cooperative Engagement Capability	●	●	●	○	●
Navy's Inertial Navigation System	●	●	◑	◑	●
Navy's PNT upgrade to Global Positioning System (GPS) based PNT Service	◑	●	●	●	●
Air Force's Resilient-Embedded GPS / Inertial Navigation System	●	●	●	●	●

● effort has business case element ◑ effort is drafting business case element ○ effort does not have business case element

Source: GAO analysis of Department of Defense information. | GAO-22-106010

In addition to the above efforts, DOD is at the advanced prototyping stage for several alternative PNT efforts, including improved clocks, and satellite systems.

DOD's overall PNT portfolio is managed by the PNT Oversight Council, a statutorily established senior-level body. However, the Council has largely prioritized modernizing the existing GPS system over alternative PNT efforts during recent meetings and has no strategic objectives or metrics to measure progress on the alternative efforts. Defined objectives and metrics would help the Council better measure overall performance and mitigate any potential gaps in PNT capabilities as the military transitions to using M-code.

Contents

Tables

Figures

Abbreviations

ACNS	Automated Celestial Navigation System
ALTNAV	Alternative Navigation
APWM	Assured Precision Weapons and Munitions
CEC	Cooperative Engagement Capability
CIO	Chief Information Officer
CUI	Controlled Unclassified Information
DAPS	Dismounted Assured Positioning Navigation and Timing System
DOD	Department of Defense
EMB	Executive Management Board
GHOST	Global Positioning System based Positioning, Navigation, and Timing Service Hull Optimized System Tactical
GPNTS	Global Positioning System based Positioning, Navigation, and Timing Service
GPS	Global Positioning System
INS	Inertial Navigation System
PNT	positioning, navigation, and timing
M-code	Military code
MAPS	Mounted Assured Positioning, Navigation and Timing System
MOSA	modular open systems approach
N/A	not available
NASA	National Aeronautics and Space Administration
NTS-3	Navigation Technology Satellite – 3
PMI	Project Management Institute
R-EGI	Resilient-Embedded Global Positioning System / Inertial Navigation System
USSPACECOM	United States Space Command

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

August 5, 2022

The Honorable Jack Reed
Chairman
The Honorable James M. Inhofe
Ranking Member
Committee on Armed Services
United States Senate

The Global Positioning System (GPS)—consisting of satellites, ground control systems, and end user receivers—provides accurate position, navigation, and timing (PNT) data to military and civilian users, but multiple threats can render those data unavailable or inaccurate. Adversaries have the ability to disrupt or deny the capabilities provided by GPS. Given its ubiquity, the denial or disruption of GPS capabilities could impact aircraft, ships, munitions, land vehicles, and ground troops in military operations and conflicts. For instance, in 2017 the installation of a new system at the San Angelo Airport interrupted civilian GPS systems for both ground and air operations within 15 miles.

The Department of Defense (DOD) recognizes the threats to GPS and is taking steps to address them. Since the late 1990s, DOD has been developing a new, more robust GPS capability known as military code, or M-code. While M-code is a stronger signal with more advanced encryption, its development has been underway for more than a decade, with initial operational capability still years away. Additionally, DOD is pursuing alternative PNT technologies that are not dependent on GPS signals being continuously available.

Congress has recognized the importance of GPS in providing PNT data. For example, the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 directed the Secretary of Defense to mature, test, and produce alternative PNT equipment for prioritized mission elements within 2 years of the legislation's enactment.[1]

Given the potential for alternative technologies to help improve access to PNT information if GPS becomes unavailable, you asked us to review

[1] William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 1611, 134 Stat. 3388, 4048-49 (enacted on January 1, 2021) (codified at 10 U.S.C. § 2281 note).

DOD's alternative PNT efforts. This report (1) identifies the threats that require DOD to invest in other navigation solutions, (2) identifies alternate PNT programs or efforts currently under development for defense applications and assesses the status of the effort's business case, and (3) assesses how DOD is overseeing the development of the alternative PNT capabilities.

This report is a public version of a sensitive report that we issued on April 6, 2022.[2] DOD deemed some of the information in our April 2022 report to be sensitive, which must be protected from public disclosure. Therefore, this report omits sensitive details about seven of the 11 alternative PNT technology and product development efforts we identified. Although the information provided in this report is more limited, the report addresses the same objectives as the sensitive report and uses the same methodology.

To identify the threats to GPS, we reviewed research available on threats to GPS, interviewed agency officials, and analyzed agency documents. To gather information on each of the alternative PNT efforts, we identified efforts based on DOD documentation and interviews. For each identified effort, we sent a questionnaire to program officials requesting information about business case documentation, budget, and timelines. For select alternative PNT efforts, we assessed questionnaire responses to determine if these efforts had a complete business case.[3] For more information on our questionnaire, see Appendix I. To determine how DOD is overseeing PNT, we evaluated DOD documents and conducted interviews to understand the oversight structure. We assessed this information against portfolio management best practices.[4] We also analyzed the meeting minutes from the body charged with oversight of DOD's PNT efforts, known as the PNT Oversight Council, to determine the main focus of those meetings. We reviewed both classified and unclassified sources, but have focused on unclassified sources to

[2] GAO, *GPS ALTERNATIVES: DOD Is Developing Navigation Systems But Is Not Measuring Overall Progress*, GAO 22-104609SU (Washington, D.C.: Apr. 6, 2022).

[3] Specifically, we were looking for the following elements of a business case: requirements, acquisition strategy, assessment of technical risk, assessment of schedule risk, and an independent cost estimate. For more information on business cases, see *Acquisition Reform: DOD Should Streamline Its Decision-Making Process for Weapon Systems to Reduce Inefficiencies,* GAO-15-192 (Washington, D.C.: Feb. 24, 2015).

[4] Project Management Institute, Inc., *The Standard for Portfolio Management*, 4th ed. (2017).

produce an unclassified report. Appendix I provides additional information on our scope and methodology.

We conducted this performance audit from November 2020 to April 2022 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We subsequently worked with DOD from April 2022 to August 2022 to prepare this public version of the sensitive report. This public version was also prepared in accordance with these standards.

Background

Department of Defense GPS Enterprise

American military and civilian users depend on assured PNT information, which is essential to effective military operations and civil infrastructure. GPS is the primary source of PNT information for U.S. and multinational warfighters and is operated by the U.S. Space Force on behalf of DOD.[5]

GPS consists of three segments:

- A space segment consisting of a constellation of 31 medium Earth orbiting satellites that continuously broadcast position and time data,[6]
- A ground control segment for commanding and controlling the satellites, and
- A user segment, comprised of receivers used by civilians and the military in aircraft, ships, land vehicles, munitions, and handheld devices.

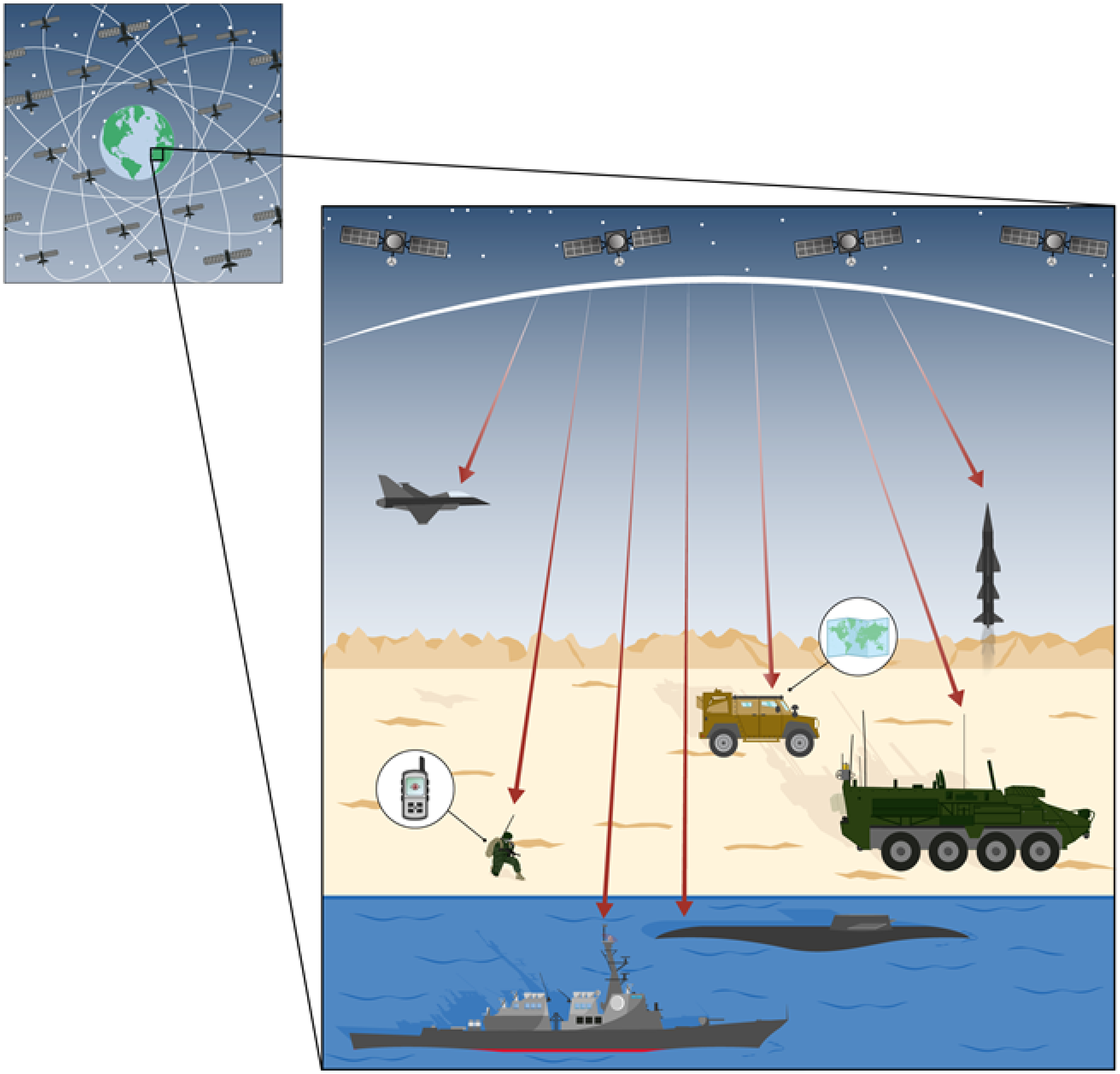
[5] The U.S. Space Force is a branch of the Armed Forces established on December 20, 2019, within the Department of the Air Force. See United States Space Force Act, Pub. L. No. 116-92, §§ 951-961, 133 Stat. 1211, 1561-68 (2019).

[6] Earth orbits include low, medium, and high orbits and determine how quickly satellites move around the Earth. Low Earth orbit is 180-2,000 km above the Earth. Medium Earth orbit is 2,000-35,780 km above the Earth. High Earth orbit is greater than 35,780 km above the Earth.

DOD began developing a space-based navigation satellite constellation in the 1970s. The system was initially available only to U.S. Navy vessels using large receivers. By the 1991 Persian Gulf War, GPS equipment was small and inexpensive enough to also be used on military vehicles. Since then, further advances, such as the development of even smaller microchip-sized receivers, have allowed GPS to provide precise PNT information for individual soldiers, munitions, military weapons and technology, and civilian applications, like smartphones.

DOD has a variety of platforms, such as bombers, unmanned vehicles, surface ships, submarines, munitions, soldiers in vehicles, and soldiers on foot. Each platform has varying constraints on the cost, size, weight, and power of its particular PNT systems. For example, an aircraft carrier can accommodate PNT systems with higher cost, larger size and weight, and greater power requirements than would be appropriate for a soldier on foot. Furthermore, the various platforms have varying missions and operating environments. For example, a fighter aircraft maneuvering in combat would have different PNT requirements than a submarine below the water's surface. Figure 1 shows different uses by U.S. military forces of the GPS satellite constellation.

Figure 1: Global Positioning System Operational System



Source: GAO analysis of DOD information. | GAO-22-106010

DOD has been in the process of modernizing the GPS enterprise since the late 1990s. The ongoing GPS acquisition efforts aim to (1) modernize and sustain the existing GPS capability, and (2) enhance the current GPS system by adding a more robust anti-jam, anti-spoof, cybersecure M-code

GPS capability as part of GPS modernization.[7] The current military signal is an encrypted signal, while the civilian signal is unencrypted. This encryption is intended to prevent unauthorized use and make the signal more difficult to disrupt. M-code is a more robust, more securely encrypted, military-specific GPS signal designed to meet military PNT needs. While M-code uses a more powerful signal and protects against false GPS signals through encryption, our prior work has shown that the GPS modernization programs have experienced significant schedule delays and cost increases.[8] In addition to M-code, DOD is using anti-jam antennas to reduce the threat of jamming. These antennas can either selectively filter out some radio frequencies coming from certain directions, selectively boost the signal coming from the direction of the GPS satellites, or both.

Alternative PNT as a Response to GPS Threats

With DOD's increased reliance on GPS satellites, this single source of PNT data becomes a more attractive target for adversaries seeking to disrupt or deny access to GPS signals. According to DOD's Office of the Under Secretary of Defense for Research and Engineering, in order to mitigate the threats to GPS, "a diverse array of technologies is required to meet current and future DOD PNT requirements."[9] We reported in 2021 that DOD was pursuing efforts to complement GPS with several alternative PNT technologies and examined several of them to assess how DOD plans to meet future PNT needs.[10] DOD's intent in using this approach is that these alternative sources would work together, even when GPS is available, to check the accuracy of each source, including GPS, and combine information if the quality of a single source degrades.

[7] Anti-jam capability blocks signal interference (jamming). Anti-spoof capability protects users against false signals that adversaries may employ to imitate friendly GPS systems (spoofing).

[8] GAO, *GPS Modernization: DOD Continuing to Develop New Jam-Resistant Capability, But Widespread Use Remains Years Away,* GAO-21-145 (Washington, D.C.: Jan. 19, 2021).

[9] Department of Defense, Office of the Under Secretary of Defense for Research and Engineering, *2020 Positioning, Navigation, and Timing Science and Technology Roadmap* (Alexandria, Va.: July 2020).

[10] GAO, *Defense Navigation Capabilities: DOD is Developing Positioning, Navigation, and Timing Technologies to Complement GPS,* GAO-21-320SP (Washington, D.C.: May 10, 2021).

DOD seeks to develop alternative PNT technologies with three characteristics.

- Robust. Robust technologies have the ability to continue seamless operations with PNT information despite threats to GPS-supplied information.
- Resilient. Resilient technologies have the ability to resist, recover from, or adapt to threats.
- Integrated. Integrated technologies use an open systems approach that allows changes to system components throughout the system lifecycle to afford opportunities for enhanced competition and innovation.

DOD's alternative research and development PNT portfolio explores two technology approaches.

- Relative. Relative PNT technologies use onboard sensors to track the position of a platform and keep time without the use of an external signal.
- Absolute. Absolute PNT technologies use external sources of information, other than GPS, to determine the position of a platform, geo-referenced to Earth

Table 1 describes each PNT approach and examples of technologies currently under research and development at DOD.

Table 1: Position, Navigation, and Timing (PNT) Approaches and Examples of Technologies Currently under Research and Development at Department of Defense

Category	Approach	Potential technologies	Capabilities	Limitations
Relative PNT	Inertial sensors	Mechanical: e.g., microelectromechanical systems	New materials could improve performance and lower cost	Mechanical noise limits performance
Relative PNT	Inertial sensors	Non-mechanical: e.g., thermal beam atomic	Could exceed performance of fiber optic gyros	High precision sensor alignment makes production challenging; environmental sensitivity
Relative PNT	Clocks	Chip-scale atomic clocks	Compact and low power	Expensive and limited precision – efforts are underway to improve with algorithms and manufacturing
Relative PNT	Clocks	High precision atomic and optical clocks	Potential Global Positioning System (GPS)-level timing	Manufacturing challenges; larger size and power requirements

Category	Approach	Potential technologies	Capabilities	Limitations
Absolute PNT	Environmental maps	Celestial navigation (stars and satellites)	Day/night coverage 50 meter accuracy	Limited access to stars and satellites (e.g., clouds)
Absolute PNT	Environmental maps	Magnetic	100 meter accuracy	Need for magnetic maps; electromagnetic noise from the system platform
Absolute PNT	Environmental maps	Terrestrial image analysis (landmarks and terrain)	10 meter accuracy	Restricted by weather (e.g., clouds); need for landmarks in images
Absolute PNT	Radiofrequency-including signals of opportunity	Terrestrial: e.g., very low frequency	500 meter accuracy—sufficient for sea	Limited network; corrections for ionosphere
Absolute PNT	Radiofrequency-including signals of opportunity	Space: e.g., low Earth orbit satellites	Radiofrequency bands complementary to GPS and stronger signal	Potentially lower precision than GPS; requires many satellites for global coverage

Source: GAO analysis of Department of Defense (DOD) information. Photos obtained from DOD (inertial sensors—left, clocks), stockedup/stock.adobe.com (inertial sensors—right), Петро Сливчук/stock.adobe.com (environmental maps), and GAO analysis of DOD information (radiofrequency signals). | GAO-22-106010

DOD Acquisition Processes

DOD can conduct acquisition in several ways. Historically, new capabilities were generally acquired by DOD using policy and procedures established in DOD Instruction 5000.02. In fiscal year 2020, DOD restructured DOD Instruction 5000.02 by introducing an adaptive acquisition framework comprising six acquisition pathways, each tailored for the characteristics and risk profile of the capability being acquired.[11] Under the major capability acquisition pathway, formal acquisition programs generally proceed through a number of phases, including technology maturation and risk reduction, engineering and manufacturing development, and production and deployment. For acquisitions that require development more quickly, DOD can use other pathways that include the urgent capability acquisition pathway and the middle tier of acquisition pathway.

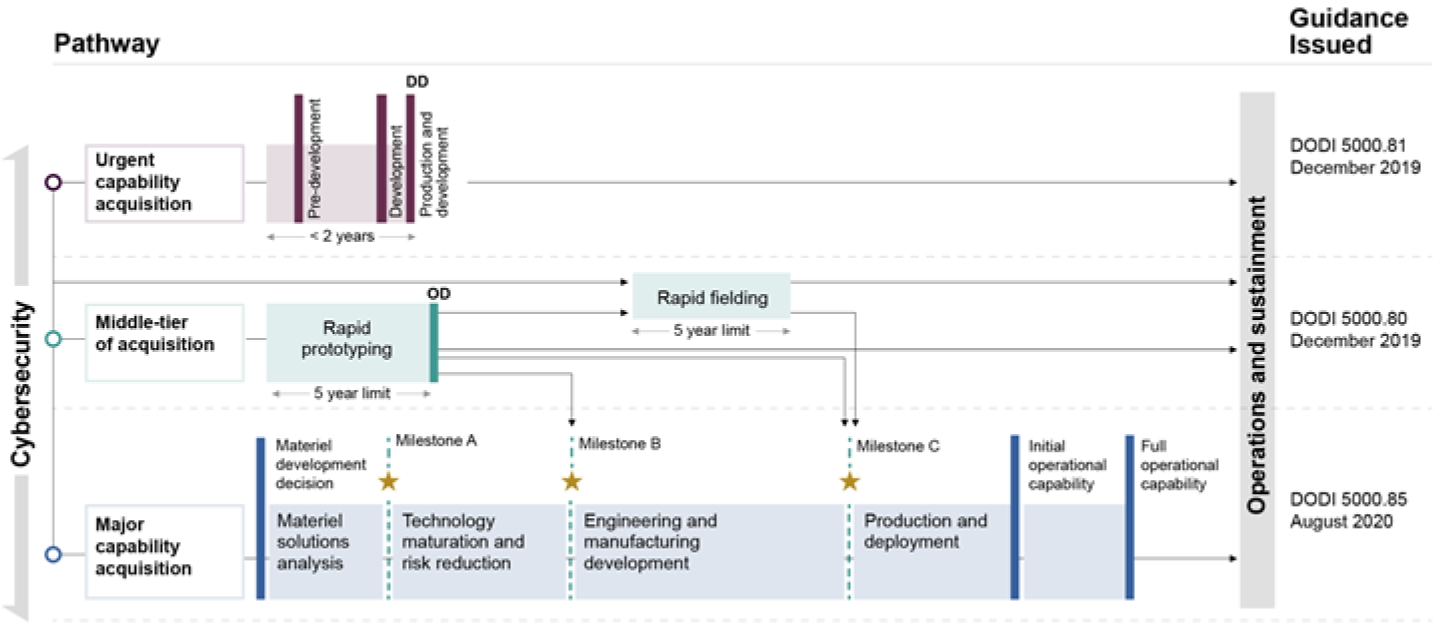
For the alternative PNT efforts described in this report, DOD uses the urgent capability acquisition, middle-tier of acquisition, or major capability acquisition pathways. Efforts following the urgent capability acquisition

[11] DOD has issued acquisition policy documents for each of the six acquisition pathways. In connection with the restructuring, the previous version of DOD Instruction 5000.02 was renumbered as DOD Instruction 5000.02T and remains in effect with content removed as it is canceled or transitioned to a new issuance. DODI 5000.02, Operation of the Adaptive Acquisition Framework (Jan. 23, 2020).

pathway provide capabilities to fulfill urgent operational needs that can be fielded in less than 2 years. The middle tier of acquisition pathway provides a streamlined acquisition process for programs intended to be completed within 2 to 5 years.[12] Programs using the middle tier of acquisition pathway and urgent capability pathway generally do not follow DOD's traditional acquisition and requirements development processes. Figure 2 shows examples of the acquisition process for these three types of acquisition pathways.

[12] The middle tier of acquisition pathway includes paths for rapid prototyping and rapid fielding efforts. The objective of a program using the rapid prototyping path is to field a prototype meeting defined requirements that can be demonstrated in an operational environment and provide for residual operational capability within 5 years of the middle tier of acquisition program start date. The objective of a program using the rapid fielding path is to begin production within 6 months and complete fielding within 5 years of the middle tier of acquisition program start date. For more information on DOD's efforts using the middle tier of acquisition pathway, see GAO, *Weapon Systems Annual Assessment: Updated Program Oversight Approach Needed,* GAO-21-222 (Washington, D.C.: June 8, 2021); and *DOD Acquisition Reform: Increased Focus on Knowledge Needed to Achieve Intended Performance and Innovation Outcomes,* GAO-21-511T (Washington, D.C.: Apr. 28, 2021).

Figure 2: Examples of the Acquisition Pathways Typically Used for Alternative Position, Navigation, and Timing Efforts


Pathway
Guidance Issued
Cybersecurity
Urgent capability acquisition
Pre-development
Development
Production and development
DD
< 2 years
DODI 5000.81 December 2019
Middle-tier of acquisition
Rapid prototyping
OD
5 year limit
Rapid fielding
5 year limit
DODI 5000.80 December 2019
Major capability acquisition
Materiel development decision
Milestone A
Milestone B
Milestone C
Initial operational capability
Full operational capability
Materiel solutions analysis
Technology maturation and risk reduction
Engineering and manufacturing development
Production and deployment
DODI 5000.85 August 2020
Operations and sustainment

OD = Outcome determination
DD = Disposition decision

Source: GAO analysis of DOD data. | GAO-22-106010

Business Cases for Acquisitions

A complete business case gives decision makers information at the start of product development to set the effort up for success. We previously identified establishing a business case as a knowledge-based leading practice that, among other leading practices, has a statistically significant correlation with improved cost and schedule performance.[13] Documentation in a business case includes the following:

- Requirements. Requirements establish what the system is to do, how well it is to do it, and how it is to interact with other systems. Without requirements, decision makers do not know if the available resources

[13] GAO, *Weapon Systems Annual Assessment: Updated Program Oversight Approach Needed,* GAO-21-222 (Washington, D.C.: June 8, 2021); and *DOD Acquisition Reform: Increased Focus on Knowledge Needed to Achieve Intended Performance and Innovation Outcomes,* GAO-21-511T (Washington, D.C.: Apr. 28, 2021).

(cost, schedule) will be sufficient to deliver a system that will meet users' needs.[14]

- Acquisition strategy. In our prior work, we found that having an acquisition strategy is key to program success, specifically in that an acquisition strategy can match requirements to resources, among other things.[15]
- Assessment of technology risk. In our prior work, we found that assessing the maturity of the technology is fundamental to managing the risk in an acquisition. These technical risk assessments can illuminate concerns and serve as the basis for realistic discussions on how to address potential risks as programs move from the early research and technology development to system development and beyond.[16]
- Assessment of schedule risk. A schedule risk analysis helps inform decision makers on the certainty of completion by a specific date, risks most likely to delay the project, and the paths or activities that are most likely to delay the program.
- Independent Cost Estimate. For cost estimates, we have previously found that optimistic program managers do not adequately allow for changes in scope, schedule delays, or other elements of risk in their program office cost estimates. To properly mitigate this optimism, it is important to have an independent view of the program, such as by DOD's Office of Cost Assessment and Program Evaluation. In the event an independent cost estimate is cost and time prohibitive, an alternative approach is to have an independent cost estimating organization outside of the program office or the program executive office conduct an independent cost assessment to validate the program office's assumptions and processes used in developing their

[14] Requirements best practices include eliciting and developing customer and stakeholder requirements; analyzing them to ensure that they will meet users' needs and expectations; and validating requirements as the system is being developed to ensure that the final system to be deployed will perform as intended in an operational environment. GAO, *Defense Major Automated Information Systems: Cost and Schedule Commitments Need to Be Established Earlier,* GAO-15-282 (Washington, D.C.: Feb. 26, 2015).

[15] GAO, *Defense Acquisitions: Better Acquisition Strategy Needed for Successful Development of the Army's Warrior Unmanned Aircraft System,* GAO-06-593 (Washington, D.C.: May 19, 2006).

[16] GAO, *Technology Readiness Assessment Guide: Best Practices for Evaluating the Readiness of Technology for Use in Acquisition Programs and Projects [Reissued with revisions on Feb. 11, 2020.],* GAO-20-48G (Washington, D.C.: Jan. 7, 2020).

cost estimate.[17] Having this “honest broker” approach to programs, helps bring to light actions that can potentially limit the organization’s ability to succeed.

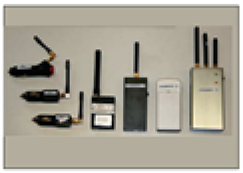
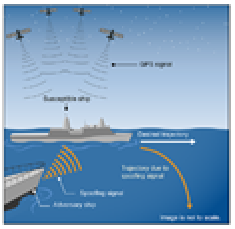
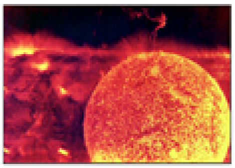
DOD has taken some steps to improve availability of business case information to decision makers. DOD acquisition policy provides opportunities for DOD officials to tailor acquisition approaches consistent with the urgency and characteristics of the capability being acquired, as well as the pathway being used. Given this flexibility, DOD officials may not require a complete business case for each program or effort.

DOD Has Identified Several Categories of Threats to GPS

While DOD recognizes that GPS will be the primary source for PNT for the foreseeable future, it also recognizes that potential threats to GPS require investments in complementary technologies. These threats can be categorized as: (1) jamming, (2) spoofing, (3) cyber, (4) unintentional interference, and (5) direct attacks on satellites or satellite infrastructure. See figure 3 for descriptions of these threats.

[17] GAO, *Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Program Costs,* GAO-20-195G (Washington, D.C.: Mar. 12, 2020).

Figure 3: Summary of Types of Selected Threats to Position, Navigation, and Timing (PNT) Tools

	Threat type	Description
	Jamming	Jamming devices are radio transmitters that intentionally block, jam, or interfere with Global Positioning System (GPS) signals.
	Spoofing	Spoofing deceives the receiver by substituting a fake GPS signal with erroneous information for the real GPS signal.
	Cyber	Cyber threats are attacks on computer systems and networks such as hacking, viruses, and denial of service that can target satellites or their ground control systems.
	Unintentional interference	Unintended interference from a variety of sources such as large geographic features (e.g. valleys and mountains), solar flares, and radio emissions on nearby frequencies can cause degradation or loss of GPS signals.
	Direct Attacks	Direct attacks on space-based satellites, such as GPS satellites, and corresponding infrastructure, such as ground control systems, can come from ground based missiles, directed energy weapons (e.g. lasers), and satellites equipped to maneuver and attack other satellites.

Source: GAO analysis of information from the Department of Defense, the Center for Advanced Defense Studies, and Center for Strategic and International Studies. Graphics obtained from United States Space Command (USSPACECOM) (jamming row), GAO analysis of DOD information (spoofing row), denisismagilov/ stock.adobe.com (cyber row), National Aeronautics and Space Administration John H. Glenn Research Center at Lewis Field (unintentional interference row), and alexyz3d/stock.adobe.com (anti-satellite row). | GAO-22-106010

Jamming Prevents the Use of GPS Signals

According to DOD's Joint Navigation Warfare Center, jamming is the most common and prevalent threat to GPS, largely because jammers are cheap and easily accessible. Jamming intentionally blocks or interferes with communications to or from receivers and transmitters (e.g., GPS satellites to GPS receivers) by transmitting higher power signals in the same radio frequency band used by GPS. For example, a 1-watt jammer, about twice the power of a LED night light, can prevent the continuous tracking of the military GPS signal at a distance of about 2 miles and can prevent the initial acquisition of that signal at about 10 miles. GPS jamming requires a direct line of sight to the target receiver, so countries employing these devices typically mount them on objects, such as tall radio towers, to maximize impact and range. Even encrypted military GPS signals can be jammed. According to reports by the Center for Strategic and International Studies, some countries use stronger, more advanced jamming systems to deny GPS access.[18] See table 2 for examples of jamming capabilities.

Table 2: Reported Examples of Jamming Capabilities

Year	Country	Jamming capability
2019	China	China has reportedly developed an aircraft equipped with Global Positioning System (GPS) jamming systems, including several new antennas and conformal electronic-warfare arrays along the fuselage.
2019	Russia	Russia announced delivery of the first units of GPS jammers to be installed on the country's 250,000 cell phone towers, intended to protect Russian assets against cruise missiles, drones, and precision-guided munitions.
2020	Iran	Islamic Revolutionary Guard Corps conducted two major exercises in 2020, which Iranian sources claim included "space operations" using jamming drones and radar units.
2020-2021	North Korea	North Korea conducted multiple jamming operations from 2020 through 2021 against South Korea focused on electronic jamming and signals reconnaissance.

Source: Center for Strategic and International Studies. | GAO-22-106010

[18] The Center for Strategic and International Studies (CSIS) is a nonprofit policy research organization. *Space Threat Assessment 2021*, Report of the CSIS Aerospace Security Project (Washington, D.C., April 2021), *Space Threat Assessment 2020*, Report of the CSIS Aerospace Security Project , (Washington, D.C., March 2020).

Spoofing Deceives GPS Receivers

According to the Center for Advanced Defense Studies, over the past decade, spoofing has become more of a concern due to the availability of cheap, commercially available and portable software-defined radios and open-source software programs capable of producing and transmitting spoofed GPS signals. A spoofing attack is designed to mimic the GPS signal, but provide erroneous information to deceive the receivers into reporting a false location. Spoofed signals are able to force vulnerable GPS receivers to disregard authentic GPS satellite signals and instead lock on to the signals generated from the spoofing device. Once a receiver locks on to the spoofed signals, the spoofing transmitter can relay false position or timing information to the receiver.

Direct spoofing of encrypted GPS signals would involve transmitting a signal that is properly encrypted. Through a spoofing attack referred to as meaconing, an adversary can spoof encrypted military GPS signals without cracking the encryption by rebroadcasting a time-delayed copy of the original signal without decrypting or altering the data. In this case, the receiver would misidentify its location because the location information it received was from an earlier period of time. While software-defined radios can be used for a variety of innocuous applications including amateur radio broadcasting, aircraft tracking, and ship tracking, they have the capability of mimicking authentic GPS satellite signals and can be obtained for under $300. See table 3 for examples of spoofing capabilities.

Table 3: Reported Examples of Spoofing Capabilities

Year	Country	Spoofing capability
2011	Iran	Iran claimed it forced a U.S. RQ-170 drone to land inside its borders by jamming its satellite communications links and spoofing its GPS receiver.
2018	Russia	A study found that Russian spoofing signals originating from Khmeimim Airbase forced some of the drones carrying explosive munitions to land at “assigned coordinates.” Khmeimim Airbase serves as one of the primary staging locations for Russian military sorties in Syria, and houses the most advanced Russian military assets deployed in Syria.
2018-2019	China	A series of incidents occurred in China’s coastal waters in which multiple ships were simultaneously spoofed to different locations. In one incident, some vessels were shown to be far inland while others showed vessels moving at very high speeds.

Source: Center for Strategic and International Studies and Center for Advanced Defense Studies. | GAO-22-106010

Cyber Threats Are Not Limited by Range

While transmitter power limits the range for jamming and spoofing attacks, the impact from cyberattacks can have far greater reach, as long as the target is accessible via a computer network, and can present a greater threat. In 2018, we found that automation and connectivity are fundamental enablers of DOD's modern military capabilities, but they make weapon systems more vulnerable to cyberattacks.[19] According to DOD and the National Aeronautics and Space Administration (NASA), cyber threats exist for all GPS segments: space, ground control, and user equipment. One study on GPS approached the system as a computer system instead of a signal system and found that the intricate nature of the GPS devices provided a large attack surface that is vulnerable to cyberattack.[20] See table 4 for other examples of cyber warfare capabilities.

Table 4: Reported Examples of Cyber Warfare Capabilities

Year	Country	Cyber warfare capability
2020	China	The U.S. Defense Intelligence Agency assessed that China could employ its cyberattack capabilities to establish information dominance in the early stages of a conflict to constrain an adversary's actions, or slow its mobilization.
2020	Russia	Russia launched a hack known as the SolarWinds Breach by gaining access through a software company's software used to manage computer systems. The attack was able to affect many U.S. federal agencies, including the Department of Defense at the Pentagon.
2020	Russia	Hackers conducted a cyberattack on Garmin's commercial GPS navigation services using a hacking tool developed by a hacking group with ties to Russia. The attack affected a wide range of Garmin services including website functions, customer support, and company communications. Additionally, pilots who use Garmin were unable to download up-to-date aviation databases before they could fly.

[19] GAO, *Weapons Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities,* GAO-19-128 (Washington, D.C.: Oct. 9, 2018).

[20] Tyler Nighswander, Brent Ledvina, Jonathan Diamond, Robert Brumley, and David Brumley, "GPS Software Attacks," Proceedings of the 2012 Association for Computing Machinery Conference on Computer and Communications Security (2012): 450-461.

Year	Country	Cyber warfare capability
2020	North Korea	Experts estimate that around 6,000-7,500 military personnel conduct cyber warfare for the North Korean state. Given its demonstrated cyber capabilities, it is conceivable that North Korea could initiate a cyberattack against U.S. space systems or ground stations, although there is no publicly available information to suggest this has happened to date.

Source: Center for Strategic and International Studies and British Broadcasting Corporation. | GAO-22-106010

Unintentional Interference Comes from Various Sources

GPS signals can unintentionally be denied or degraded due to several factors, including geography, environment, and spectrum interference. See table 5 for examples of unintentional interference.

Table 5: Examples of Unintentional Interference

Type of interference	Definition	Examples
Geography	Inability to receive a GPS signal due to interference from geographic features	In some situations, such as in a tunnel, near a mountain, or near tall buildings, a GPS receiver may not be able to receive the signal from the satellites. This will cause an outage of GPS for the user, until the user moves to an open location.
Environmental	Certain environmental conditions can cause problems with GPS signal reception	Solar flares, often accompanied by very powerful bursts of radio energy, can result in intermittent signal disruption to GPS receivers for many minutes.
Spectrum	Higher power signals in the same frequency bands GPS uses, or potentially nearby bands, may interfere with the GPS signals	According to DOD and National Aeronautics and Space Administration, degradation from signals operating in close proximity to GPS frequencies can cause reduced accuracy, an intermittent signal, or total loss of a position/timing signal that could negatively affect military operations.

Source: National Aeronautics and Space Administration, GPS World and the Congressional Research Service. | GAO-22-106010

Some Countries Can Target GPS Satellites and Infrastructure

Some countries can directly target satellites to interrupt their operations, damage, or destroy them. Anti-satellite threats can be kinetic or non-kinetic.

- Kinetic threats generally involve directing physical objects, such as missiles, to impact satellites and can originate from the ground or from objects in orbit. Ground-based kinetic threats include ground-based missiles from fixed or mobile launch systems. Orbital-based kinetic threats include satellites that are designed to physically damage or destroy other satellites. Kinetic attacks in space can result in space debris, including derelict spacecraft and remnants from explosions or collisions. Space debris can lead to further damage and destruction to other satellites and space vehicles.
- Non-kinetic threats can be directed from ground-based sites or from orbital objects and include directed energy weapons such as lasers, radiofrequency jammers, high-power microwaves, or similar tools. Non-kinetic threats can result in temporarily disabling space-based capabilities or permanently damaging them.

According to the Center for Strategic and International Studies, while no country has conducted a physical attack against another country's satellites, four countries (U.S., Russia, China, and India) have successfully tested anti-satellite weapons. In addition to direct attacks on satellites, GPS infrastructure, such as ground control stations, can also be targeted using similar means. Table 6 lists some examples of anti-satellite capabilities.

Table 6: Reported Examples of Anti-Satellite Capabilities

Year	Country	Anti-satellite capability
2008-2019	China	China has developed and launched several satellites that could be used for co-orbital counter space capabilities. Over this period, these satellites have conducted several rendezvous and proximity operations with other Chinese satellites from low earth to geostationary orbits.
2008	United States	According to news reports, the U.S. Navy shot down an inoperable satellite before it could enter Earth, which potentially would cause a release of toxic gas.
2019	Russia	Russia is likely developing an airborne anti-satellite laser weapon system to use against space-based missile defense sensors.
2019	India	India conducted a successful direct-ascent anti-satellite test. An India official stated the anti-satellite weapon is capable of reaching most satellites in low earth orbit.
2020	Russia	U.S. Space Command reports Russia tested a potential co-orbital anti-satellite system consisting of a satellite that maneuvered near and fired a small projectile at another Russian satellite.

Source: Defense Intelligence Agency and Center for Strategic and International Studies. | GAO-22-106010

Given DOD's reliance on GPS, these threats have the potential to limit the military's ability to conduct operations. While the impact of these threats can deny or degrade GPS, some DOD platforms may be able to continue to operate without GPS for a period of time, but as GPS degradation or denial stretches on, more missions will be impacted.

Military Services Are Developing Alternative PNT Capabilities, but Some Efforts Have Incomplete Acquisition Business Cases

DOD is developing systems able to incorporate multiple PNT sources simultaneously using an open systems approach to facilitate the ability to incorporate new technologies. We identified 11 efforts aimed at providing alternatives to GPS. Five of the 11 current alternative PNT efforts are either using a major capability acquisition pathway or a middle tier of acquisition pathway, but four of those efforts lack complete business case documentation. Of the six remaining efforts, the business case best practice does not apply, but three of these efforts are in the process of preparing business cases.

DOD Plans to Field PNT Capabilities Using a Modular Open Systems Approach

DOD is pursuing multiple different types of PNT capabilities to keep up with emerging threats to GPS and developing systems able to incorporate multiple PNT sources simultaneously. DOD officials have asserted that DOD must integrate and field new PNT capabilities more rapidly. For example, we previously reported that the military services have taken more than a decade to transition from current GPS equipment to M-code equipment capable of receiving a stronger, more securely encrypted GPS signal. Further, the cost to transition will likely be billions of dollars greater than the $2.5 billion identified through fiscal year 2021, because significant work remains.[21] Additionally, current PNT receivers are not designed to easily add in new sources of PNT information. We reported in

[21] GAO, *GPS Modernization: DOD Continuing to Develop New Jam-Resistant Capability, But Widespread Use Remains Years Away,* GAO-21-145 (Washington, D.C.: Jan. 19, 2021); and *Global Positioning System: Better Planning and Coordination Needed to Improve Prospects for Fielding Modernized Capability,* GAO-18-74 (Washington, D.C.: Dec. 12, 2017).

2021 that such PNT receivers are a challenge to fielding new capabilities, as these systems cannot be upgraded affordably.[22]

To address these challenges, DOD's strategy is to use a modular open systems approach (MOSA) as much as possible.[23] This approach incorporates modular design and open standards for key interfaces and can readily accept data from alternative PNT sources from a variety of suppliers without redesigning the entire system.

One key part of the open systems approach is DOD's development of receivers that can receive and use multiple sources of PNT information, which we refer to as "multi-PNT receivers." These multi-PNT receivers are intended to be capable of integrating multiple sources of PNT, including GPS M-code as well as alternative PNT data sources. Multi-PNT receivers add resiliency to a warfighter's mission by providing multiple sources of PNT information which allows the warfighter to continue their mission with minimal, or even no degradation, should one of the PNT sources be unavailable for a period of time. These receivers are also being built to more easily add future alternative PNT capabilities.

In simplified terms, a multi-PNT receiver is a box that is placed on a platform, such as a ship. The box would contain multiple PNT receiver cards, with different PNT capabilities, which can be installed and changed out depending on the PNT capability needed. The box may also receive information from other components on the platform, such as antennas for a radiofrequency signal or acceleration and rotation data from an inertial measurement sensor.

The multi-PNT receiver manages and analyzes the various sources of PNT information to determine the position, velocity, and orientation of the platform. For example, the Army's multi-PNT receiver for vehicles, called the Mounted Assured Positioning, Navigation and Timing System (MAPS), plans to integrate the following PNT sources:

- M-code capable GPS receiver

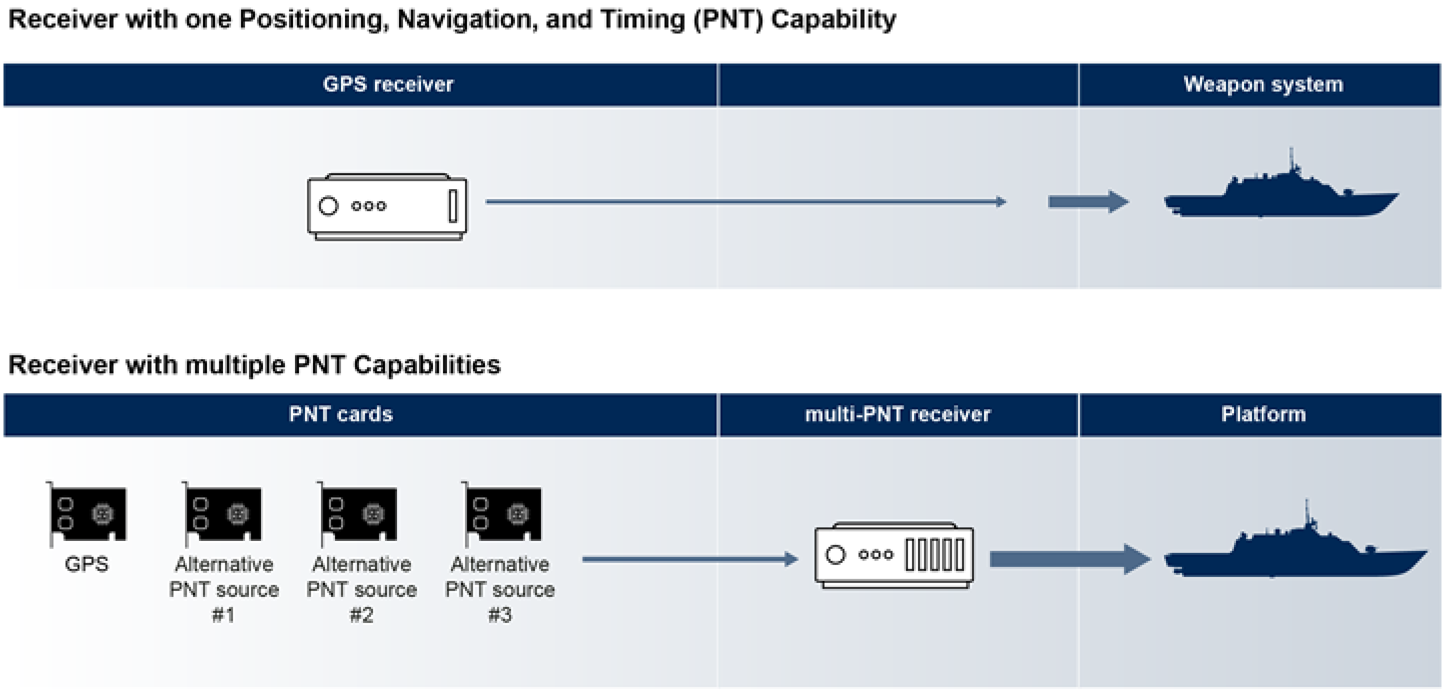
[22] GAO, *Defense Navigation Capabilities: DOD is Developing Positioning, Navigation, and Timing Technologies to Complement GPS,* GAO-21-320SP (Washington, D.C.: May 10, 2021).

[23] DOD, *Strategy for the Department of Defense Positioning, Navigation, and Timing (PNT) Enterprise*, (Washington, DC: November 2018).

- Receiver for a commercial space based satellite system (called ALTNAV),
- Clock
- Inertial sensor that uses equipment to detect acceleration and rotation changes to measure position

Figure 4 shows how various cards with different PNT capabilities can be included in a multi-PNT receiver for a platform.

Figure 4: A traditional GPS Receiver with One PNT Capability Compared to a Multi-PNT Receiver


Receiver with one Positioning, Navigation, and Timing (PNT) Capability
GPS receiver
Weapon system
Receiver with multiple PNT Capabilities
PNT cards
multi-PNT receiver
Platform
GPS
Alternative PNT source #1
Alternative PNT source #2
Alternative PNT source #3

Source: GAO analysis and representation of Department of Defense documentation. | GAO-22-106010

The military services have four efforts underway to implement MOSA in their multi-PNT receivers for selected platforms and users (see table 7). Appendix II contains more details about each of the four multi-PNT receiver efforts.

Table 7: Efforts Underway to Implement an Open Architecture to Allow for Easier Integration of Positioning, Navigation, and Timing (PNT) Capabilities

Military service	Multi-PNT receiver	Estimated Funding 2017-2025 (in millions)	Platform or end user	PNT capabilities	Initial operational capability time frame (in fiscal year) and acquisition pathway
Army	Dismounted Assured Position Navigation and Timing System (DAPS)	$160	Troops on foot	• Global Positioning System (GPS) M-code[a] • Inertial sensor • Clock • Receiver for a space-based PNT source (ALTNAV)[b]	• 2024 • Major Capability Acquisition
Army	Mounted Assured Positioning, Navigation and Timing System (MAPS)	$480	Combat vehicles	• GPS M-code • Inertial sensor • Clock • Receiver for a space-based PNT source (ALTNAV)	• 2024 • Major Capability Acquisition
Navy	Upgrade to Global Positioning System (GPS) based Positioning, Navigation, and Timing Service (GPNTS)	$18	Surface ships	• GPS M-code • Clock • Receiver for time information from satellites • Time information from a sensor network • Automated celestial navigation	• 2022 • Major Capability Acquisition
Air Force	Resilient-Embedded Global Positioning System (GPS) / Inertial Navigation System (INS) (R-EGI)	$317	Air platforms, initial fielding on F-16s	• GPS M-code • Inertial sensor • Future alternative PNT capabilities	• N/ A[c] • Middle Tier of Acquisition

Source: GAO analysis of Department of Defense information. | GAO-22-106010

[a] M-code is a stronger, more secure GPS signal for the military.

[b] ALTNAV is an Army effort to use an existing commercial satellite constellation for PNT.

[c] Not available, the Air Force does not have an Initial Operational Capability date for R-EGI.

To implement MOSA, DOD and the military services are creating guidelines, called reference architectures. The Army and Navy have each developed a service-level PNT reference architecture that defines a MOSA for PNT, and the Air Force plans to develop its own.[24] To standardize the common elements across the individual military services'

[24] A reference architecture is an authoritative source of information about a specific subject area (in this case PNT) that guides and constrains the instantiations of multiple architectures and solutions.

reference architectures, the Army is leading an effort on behalf of the Office of the Under Secretary of Defense for Research and Engineering to draft a DOD-wide MOSA PNT reference architecture. According to officials, the DOD reference architecture is at a higher level than the military services' reference architectures, to reduce the potential for conflict between them. A draft version of the DOD-wide MOSA was released in October 2021. Army officials leading the Office of the Under Secretary of Defense for Research and Engineering MOSA effort expressed concern that funding to support the architecture process will run out in 2021. The Office of the Under Secretary of Defense for Research and Engineering is determining a path forward for PNT MOSA efforts.

Through using MOSA in PNT, DOD seeks to capitalize on cost savings, schedule reductions, more rapid deployment of new technologies, and increased interoperability. However, we found there are considerations that can affect the development and use of a MOSA in PNT, such as acceptance by the relevant communities, system performance, cybersecurity, certification, and governance and sustainment.[25]

An Open Interface Standard for Positioning Navigation and Timing (PNT)

As part of the Modular Open Source Architecture initiative, the Department of Defense (DOD) is in the process of updating a PNT interface standard, called the All-Source Positioning and Navigation standard. The standard focuses on the properties of the data messages that DOD PNT sources both send and receive. For example, the standard could require all PNT sources to send altitude measurements in meters above sea level. Currently, PNT measurements are based on the preference of an individual platform, which can be a hurdle to interoperability. The Army officials leading the standard effort are meeting with the military services and other key stakeholders, such as industry, to get buy-in on the standard.

Source: GAO-21-320SP and Department of Defense information. | GAO-22-106010

[25] For a more detailed explanation of the opportunities and considerations of using a PNT MOSA, see *Defense Navigation Capabilities: DOD is Developing Positioning, Navigation, and Timing Technologies to Complement GPS,* GAO-21-320SP (Washington, D.C.: May 10, 2021).

Military Services Are Pursuing Several Alternative PNT Efforts

In addition to the four multi-PNT receiver efforts underway, we identified seven other alternative PNT efforts. These efforts are at different stages in technology and product development.

In addition to upgrades to GPS-based PNT Service (GPNTS) multi-PNT receiver described above in table 7, the Navy has three other PNT efforts it is developing using the major capability acquisition pathway.[26] These efforts are:

1. Automated Celestial Navigation System (ACNS),
2. PNT Upgrade to the Cooperative Engagement Capability (CEC), and
3. AN/WSN-12 Inertial Navigation System.

The Army, Air Force, and DOD have four other PNT efforts, which are not yet mature enough to enter the Defense acquisition system. The Army's efforts are:

4. Alternative Navigation (ALTNAV), and
5. Assured Precision Weapons and Munitions (APWM).

The Air Force effort is:

6. Navigation Technology Satellite -3 (NTS-3).

The DOD effort is:

7. Critical Time Dissemination.

This report omits sensitive information about these seven alternative PNT efforts.

[26] The Navy is also working on a smaller form factor version of GPNTS called GPNTS Hull Optimized System – Tactical (GHOST).

DOD Has Incomplete Business Cases for Four out of Five PNT Acquisition Efforts

Five of the 11 alternative PNT efforts identified and listed above, are efforts using either the major capability acquisition pathway or the middle tier of acquisition pathway, but most lack complete business cases.[27] In particular, of the five acquisition efforts, four have incomplete business cases. The Air Force's R-EGI effort has all the elements of a business case. However, the Navy's four efforts have incomplete business cases. As shown in table 7, the Navy's GPNTS upgrade, ACNS, CEC, and AN/WSN-12 are either missing or have not completed at least one or more elements of a business case.

Table 8: Status of Business Case Documents for Department of Defense (DOD) Efforts That Have Started Development

Effort **Military Service** **Acquisition Pathway**	**Requirements documentation**	**Acquisition strategy**	**Assessment of technology risk**	**Assessment of schedule risk**	**Independent cost estimate**
Effort: Automated Celestial Navigation System (ACNS) **Military Service:** Navy **Acquisition Pathway:** Major Capability Acquisition	business case element	business case element	no business case element	no business case element	business case element
Effort: PNT upgrade to Cooperative Engagement Capability (CEC) **Military Service:** Navy **Acquisition Pathway:** Major Capability Acquisition	business case element	business case element	business case element	no business case element	business case element
Effort: AN/WSN-12 Inertial Navigation System — Replacement **Military Service:** Navy **Acquisition Pathway:** Major Capability Acquisition	business case element	business case element	drafting business case element	drafting business case element	business case element
Effort: PNT upgrade to Global Positioning System (GPS) based Positioning, Navigation, and Timing (PNT) Service (GPNTS) **Military Service:** Navy **Acquisition Pathway:** Major Capability Acquisition	drafting business case element	business case element	business case element	business case element	business case element

[27] The Middle Tier of Acquisition pathway is intended to rapidly develop fieldable prototypes to demonstrate new capabilities, rapidly field production quantities of systems with proven technologies that require minimal development, or both. We excluded two efforts—MAPS and DAPS—using the urgent capability pathway. These two efforts plan to transition to the major capability acquisition and are discussed in the next section.

Effort **Military Service** **Acquisition Pathway**	**Requirements documentation**	**Acquisition strategy**	**Assessment of technology risk**	**Assessment of schedule risk**	**Independent cost estimate**
Effort: Resilient-Embedded Global Positioning System (GPS) / Inertial Navigation System (INS) (R-EGI) **Military Service:** Air Force **Acquisition Pathway:** Middle Tier of Acquisition	business case element	business case element	business case element	business case element	business case element

Legend: ● effort has business case element, ◑ effort is drafting business case element, ○ effort does not have business case element

Source: GAO analysis of DOD information. | GAO-22-106010

For all four Navy efforts already approved to start as acquisition programs, the business case is incomplete, missing at least one of the business case documents. Specifically:

- For ACNS, the Navy does not have, and does not plan to assess technical or schedule risk.
- For the CEC upgrade, the Navy said it had not assessed schedule risk and did not plan to do so.
- For AN/WSN-12, the Navy is in the process of assessing schedule risk. Program officials stated instead of conducting a technology risk assessment, they decided to leverage the technology risk assessment of a similar system to the AN/WSN-12, but said they did not document this decision.
- For the PNT upgrade to GPNTS, the Navy is currently drafting requirements.

Since DOD acquisition policy allows DOD officials to tailor acquisition approaches based on the urgency and characteristics of the capability being acquired, as well as the pathway being used, DOD officials may decide not to require a complete business case for each program or effort. In our previous work, we have identified several knowledge-based acquisition leading practices DOD could use to improve its acquisition outcomes.[28] One such leading practice is completing the program's business case prior to starting development of an acquisition program. A complete business case includes documents that provide information to assist decision makers. For example, a technology risk assessment documents the maturity level of the technology at the start of an effort and identifies risks to maturing key technologies and efforts to mitigate those risks. Similarly, an independent cost estimate, or independent cost

[28] GAO, *Best Practices: Using A Knowledge-Based Approach To Improve Weapon Acquisition,* GAO-04-386SP (Washington, D.C.: Jan. 2004).

assessment, documents, or validates, the estimated cost of the system's desired capabilities.

The information in a complete business case can help decision makers in DOD and Congress oversee acquisition efforts. With a complete business case, decision makers can better ensure that the necessary resources are available to match the program's requirements, and that technologies used in a system will work as expected. Without a complete business case, as is the case with the four Navy efforts, DOD assumes more risk, which may result in reduced capabilities of the eventual system, delayed delivery of PNT capabilities to the warfighter, or unexpected cost increases.

DOD Is Drafting Business Cases for Three Efforts That Plan to Transition to the Major Capability Acquisition Pathway Soon

Of the six efforts not already using the major capability acquisition pathway or the middle tier of acquisition pathway, three are early stage prototyping efforts, and three are nearing a decision to transition to the major capability acquisition pathway. For the early prototyping alternative PNT efforts—NTS-3, ALTNAV, and APWM—we would not expect a business case until, if successful, the efforts transition to certain acquisition pathways such as the major capability acquisition pathway. Of the three efforts that plan to transition to the major capability acquisition pathway in fiscal year 2022 or fiscal year 2023, we found they have partial business cases (see table 8), which is expected based on the maturity of the efforts.

Specifically, the Army authorized rapid prototyping for MAPS and DAPS, which are currently using an urgent capability pathway.[29] The Army plans to transition these efforts into the major capability acquisition pathway, transitioning MAPS in fiscal year 2022 and DAPS in fiscal year 2023. Also, the DOD Chief Information Officer plans to transition the critical time dissemination effort to the major capability acquisition pathway in fiscal year 2022. As these efforts mature, we would expect officials to draft or

[29] For MAPS and DAPs, the Army is using directed requirements, which authorize a prototyping effort. The directed requirements do not replace the Joint Capabilities Integration and Development System process, but, rather, direct requirements and activities that inform and refine future Joint Capabilities Integration and Development System documents.

complete business case elements, so that a complete business case can support the decision to transition from a prototyping effort to the major capability acquisition pathway.

Table 9: Status of Business Case Documents for Department of Defense (DOD) Efforts Close to Transitioning to Major Capability Acquisition Pathway

Effort	Requirements documentation	Acquisition strategy	Assessment of technology risk	Assessment of schedule risk	Independent cost estimate
Mounted Assured Positioning, Navigation and Timing System (MAPS) Army	business case element	business case element	business case element	drafting business case element	drafting business case element
Dismounted Assured Position Navigation and Timing System (DAPS) Army	business case element	drafting business case element	drafting business case element	business case element	drafting business case element
Critical Time Dissemination DOD Chief Information Officer (CIO)[a]	drafting business case element	no business case element	business case element	no business case element	no business case element

Legend: ● effort has business case element, ◑ effort is drafting business case element, ○ effort does not have business case element

Source: GAO analysis of DOD information. | GAO-22-106010

[a] DOD Chief Information Officer is leading the effort supported by the Navy and Defense Information Systems Agency (DISA).

DOD officials in charge of these efforts are currently drafting elements of the business cases. For both the MAPS and DAPS efforts, the Army has either completed, or is drafting, all of the elements of a business case. For the Critical Time Dissemination effort, DOD CIO is drafting requirements and has completed a technology risk assessment. However, DOD CIO has not started the other documents that are part of a complete business case.

DOD's efforts to develop multiple alternate PNT efforts have interdependencies that could impact the overall effort. If one effort is delayed or has technical problems, it would likely affect DOD's overall ability to have resilient PNT. For example, the Army MAPS program (a multi-PNT receiver) integrates an ALTNAV receiver card, but the capability is partly dependent on Army's ALTNAV program to build out the ground segment.

DOD Has a PNT Oversight Structure, but Has Not Set Clear Objectives for Alternative PNT

DOD Has Established a PNT Oversight Council Including Senior Leadership and Service-Level Members

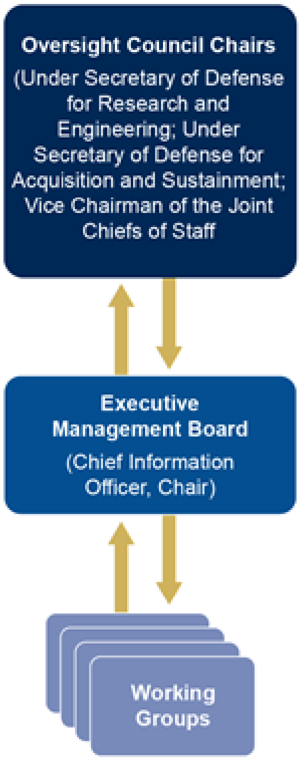
DOD established the PNT Oversight Council[30] in 2016, in response to a 2015 statute.[31] The statute established the Oversight Council to be responsible for oversight of DOD's PNT enterprise and pointed to several specific responsibilities including, vulnerability assessments and mitigation of risks as well as resource prioritization. The Oversight Council is comprised of three levels of leadership: the Chairs, which are represented by the Under Secretary of Defense for Research and Engineering, the Under Secretary of Defense for Acquisition and Sustainment, and the Vice Chairman of the Joint Chiefs of Staff;[32] the Executive Management Board, chaired by DOD's Chief Information Officer; and six working groups focusing on different aspects of PNT. See figure 5 for an organizational chart. The Chairs and Executive Management Board meet quarterly to align with the budgeting cycle, and the working groups meet at least monthly, as required to support the Chairs and Executive Management Board.

[30] "PNT Oversight Council" will be referred to as "Oversight Council" for the remainder of the report.

[31] National Defense Authorization Act for Fiscal Year 2016, Pub. L. No. 114-92, § 1603(a), 129 Stat. 1096 (2015) (codified as amended at 10 U.S.C. § 2279b).

[32] As originally enacted, the statute established two co-chairs: the Under Secretary of Defense for Acquisition, Technology, and Logistics, and the Vice Chairman of the Joint Chiefs of Staff. In connection with the reorganization of the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, the statute was amended in 2019 to establish three co-chairs, as described above. See National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, § 902(31), 133 Stat. 1198, 1546 (2019) (codified as amended at 10 U.S.C. § 2279b). At present, DOD Directive 4650.05—which establishes policy and assigns responsibilities for the DOD PNT Enterprise—does not reflect this change to the composition of the PNT Oversight Council. However, DOD officials report that DOD is updating DOD Directive 4650.05 to reflect the change, and that the Under Secretary of Defense for Research and Engineering is expected to participate in PNT Oversight Council meetings as a tri-chair beginning in fiscal year 2022.

Figure 5: Position, Navigation, and Timing (PNT) Oversight Council Organizational Chart


Oversight Council Chairs
(Under Secretary of Defense for Research and Engineering; Under Secretary of Defense for Acquisition and Sustainment; Vice Chairman of the Joint Chiefs of Staff
Executive Management Board
(Chief Information Officer, Chair)
Working Groups

Source: GAO analysis of Department of Defense information. | GAO-22-106010

The Oversight Council serves as the principal unified and integrated governance body that ensures the DOD PNT Enterprise functions meet national defense objectives, which as of 2018 included meeting the challenges posed by a re-emergence of long-term strategic competition with China and Russia.[33] Specific functions include oversight of the DOD PNT Enterprise, and identification and mitigation of vulnerabilities, such as GPS spoofing. The Oversight Council also supports the planning, programming, budgeting, and execution process by prioritizing PNT issues and recommending resourcing options.

[33] According to the DOD Strategy for the PNT Enterprise, the PNT Enterprise encompasses governance, capabilities, applications, and effects. It includes sources of PNT information, 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 Navigation Warfare Operations.

The Executive Management Board and Working Groups include representatives from the military services. Each military service has a group that coordinates its alternative PNT efforts and represents its respective military service at Oversight Council meetings.[34] According to officials, coordination on alternative PNT efforts is conducted primarily at the service-level during working group meetings and informal monthly check-ins.

PNT Oversight Council Has Largely Prioritized GPS Modernization over Alternative PNT Efforts

Although the Oversight Council has responsibility for DOD's overall PNT enterprise, it has largely prioritized GPS modernization over alternative PNT efforts. DOD officials acknowledge that GPS modernization and alternative PNT technologies are considered part of the same PNT Enterprise portfolio. The Project Management Institute (PMI) has established standards for portfolio management that are generally recognized as leading practices and used worldwide by private companies, nonprofit organizations, and others.[35] These leading practices state that portfolio management focuses on products collectively at an enterprise level, such as the PNT Enterprise, and involves evaluating, selecting, prioritizing, and allocating limited resources to projects that best accomplish strategic or organizational goals.[36]

As the manager of the PNT Enterprise portfolio, the Oversight Council has focused on GPS modernization efforts. In May 2021, we reported that officials from across DOD believe that alternative PNT solutions are not prioritized across DOD.[37] More recently, Oversight Council officials explained that alternative PNT is a relatively new issue and that DOD's

[34] The Army and Air Force have PNT cross-functional teams, while the Navy's PNT efforts are coordinated by the Navigator of the U.S. Navy.

[35] The Project Management Institute is a not-for-profit association that provides global standards for, among other things, project and program management. These standards are utilized worldwide and provide guidance on how to manage various aspects of projects, programs, and portfolios.

[36] Project Management Institute, Inc., *The Standard for Portfolio Management*, 4th ed. (2017).

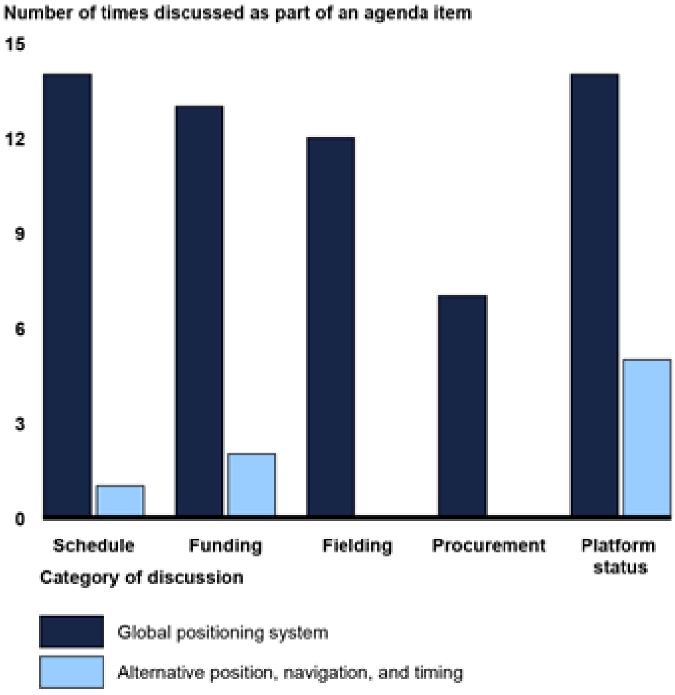
[37] GAO, *Defense Navigation Capabilities: DOD is Developing Positioning, Navigation, and Timing Technologies to Complement GPS,* GAO-21-320SP (Washington, D.C.: May 10, 2021).

focus is shifting from GPS modernization to alternatives as GPS threats become more common.

In our examination of meeting minutes, we found the PNT Oversight Council only rarely addressed alternative PNT efforts. In particular, we reviewed meeting minutes from six Oversight Council Chair meetings from 2020 and 2021.[38] During these meetings the Oversight Council members set priorities for developing PNT technologies, including GPS and alternative PNT. The meeting minute agenda items covered a range of topics; we used a content analysis to identify five common categories of topics. We found nearly all the topics of discussion were related to GPS, not alternative PNT efforts. Figure 6 shows these categories as well as the number of times that agenda items in one of these categories involved either GPS or alternative PNT. Alternative PNT was most frequently involved in agenda items that we identified as related to platform status, such as REG-I. However, the Oversight Council did not discuss alternative PNT in the context of agenda items that we identified as related to procurement or fielding. The council did discuss alternative PNT once in items that we identified as related to schedule, and twice in items we identified as related to funding.

[38] We reviewed all available Chair meeting minutes between June 2020 and August 2021 that were classified Secret. We did not review one meeting minutes from September 2020 because it was classified Top Secret.

Figure 6: Summary of Department of Defense Position, Navigation, and Timing (PNT) Oversight Council’s Discussion of GPS and Alternative PNT in 2020 and 2021 Meetings



Source: GAO Analysis of Department of Defense documentation. | GAO-22-106010

Accessible Data for Figure 6: Summary of Department of Defense Position, Navigation, and Timing (PNT) Oversight Council’s Discussion of GPS and Alternative PNT in 2020 and 2021 Meetings

na	Number of times discussed as part of an agenda item	Number of times discussed as part of an agenda item
Category of discussion	**Global positioning system**	**Alternative position, navigation, and timing**
Schedule	14	1
Funding	13	2
Fielding	12	0
Procurement	7	0
Platform status	14	5

According to DOD officials from CIO, the Oversight Council has most recently focused its efforts on addressing GPS issues due to the pressing need to purchase computer chips to support M-code receiver cards.

PNT Oversight Council Has Not Set Portfolio-Level Strategic Objectives or Metrics to Measure Progress

Although the Oversight Council has a vision, mission, and strategic goals for the PNT Enterprise, it is missing short-term strategic objectives and metrics as part of its planning. PMI's leading practices in portfolio management state that strategic planning and organizational and performance metrics are critical elements in the portfolio lifecycle.[39] These leading practices include the following as part of strategic planning:

- Vision and mission. The vision and mission describe the main purpose of an organization and its ultimate goal. A vision describes where the organization sees itself and a mission explains the overall approach for achieving this vision. They include ambitions typically 5 or more years in the future. The Oversight Council has a vision and mission, as outlined by the PNT Enterprise Strategy, to ensure resilient and trusted sources of PNT for the military and its allies.[40]
- Strategic goals. Strategic goals are general statements indicating what is to be achieved and should be integrated with the vision and mission. They are qualitative rather than quantitative targets usually 3 or more years in the future. The Oversight Council has strategic goals as described in its 2021 PNT Implementation Plan, such as continually fielding resilient PNT applications beginning in 2022.[41]
- Strategic objectives. Strategic objectives form the backbone of a strategic plan. They represent specific, short-term actions (1 to 2 years) that are the result of the vision and goals. The critical elements in a strategic objective are measurability and clarity. The Oversight Council does not have strategic objectives for how alternative PNT will meet its goal of fielding robust, resilient, and integrated PNT

[39] Project Management Institute, Inc., *The Standard for Portfolio Management*, 4th ed. (2017).

[40] Department of Defense, *Strategy for the Department of Defense Positioning, Navigation, and Timing (PNT) Enterprise* (Washington, D.C.: November 2018).

[41] Department of Defense, Implementation Plan for Resilient and Survivable Positioning, Navigation and Timing (PNT) Capabilities and Applications: Response to Section 1611 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116-283), Resilient and Survivable PNT Capabilities (Washington, D.C.: June 2021).

capabilities and the mission of providing assured PNT when GPS is either degraded or denied.

The Oversight Council developed and DOD approved an implementation plan for alternative PNT efforts in June 2021, in response to Section 1611 of the Fiscal Year 2021 National Defense Authorization Act.[42] The Act directed DOD to create a plan to generate resilient and survivable PNT capabilities for prioritized mission elements within 2 years of the legislation's enactment. We found that, although the plan includes strategic goals such as the need for alternative PNT capabilities, system priorities, service initiatives and collaboration, it does not contain strategic objectives or metrics. For example, the document states that resilient PNT applications will be fielded continually beginning in late 2022. However, there is no reference to metrics, such as specific timelines for the various alternative PNT capabilities.

The DOD PNT Enterprise mission calls for alternative PNT capabilities during operational situations when GPS is unavailable or unreliable. DOD has acknowledged that no single PNT source will support all DOD PNT requirements or be appropriate for every platform and operating environment, which is why the department is developing several alternative PNT capabilities in addition to GPS modernization. However, there are currently no strategic objectives with defined and measurable short-term actions for the development of those capabilities prior to the completion of M-code, such as a master schedule. DOD officials reported that while there is an Integrated Master Schedule tracking the development of GPS M-code, there is not a similar schedule for alternative PNT efforts.[43]

The Oversight Council should have metrics to measure progress on alternative PNT efforts, such as timelines or a schedule, since the strategic goal of these efforts is to serve in GPS-contested environments. Such environments could increasingly be the case if M-code continues to face significant schedule delays. For example, we reported in 2021 that Increment 2 of the M-code card program is already approximately a year

[42] William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 1611, 134 Stat 3388, 4048-49 (2021) (enacted on January 1, 2021) (codified at 10 U.S.C. § 2281 note).

[43] Integrated Master Schedules establish timelines for programs to achieve benchmarks and goals.

behind schedule based on design steps initially scheduled in 2018.[44] While the Oversight Council's PNT implementation plan emphasizes the need to accelerate the delivery and fielding of operational resilient PNT applications as quickly as possible, there are no timelines included for the alternative PNT capabilities. Having timelines for these capabilities would help the Oversight Council prioritize efforts, especially if capabilities need to mitigate a potential M-code capability gap.

Leading practices in portfolio management state that connecting strategic goals with performance metrics is an important part in determining how the portfolio and its components will be managed.[45] Strategic objectives and metrics at the Oversight Council level would help the Oversight Council better measure overall performance of DOD's alternative PNT efforts, which could help ensure more efficient management and consistent reporting on the status of its programs and projects at the portfolio level. This could make it easier for the Oversight Council and other decision makers to track the progress and outcomes of all programs and projects that are critical to achieving DOD's strategic PNT objectives and to better coordinate and integrate activities across the PNT Enterprise.

Conclusions

GPS has served as the primary source of navigation for military and civilian users worldwide for over two decades, but faces threats by near peers and other adversaries. These threats could put at risk the U.S. military's ability to execute its missions. DOD has identified that access to reliable PNT is critical for mission success. In response, DOD has taken steps to develop multiple alternatives to GPS and established a Council to coordinate those efforts.

The four Navy acquisition efforts using the major capability acquisition pathway are missing key documentation establishing sound acquisition business cases. A leading acquisition practice highlights the value of fully documenting business cases before beginning acquisition programs. Without complete business cases, decision makers such as the PNT

[44] GAO, *GPS Modernization: DOD Continuing to Develop New Jam-Resistant Capability, But Widespread Use Remains Years Away,* GAO-21-145 (Washington, D.C.: Jan. 19, 2021).

[45] Project Management Institute, Inc., *The Standard for Portfolio Management*, 4th ed. (2017).

Oversight Council are less informed to determine which alternative PNT capabilities will be available and when, and if those PNT capabilities remain capable of countering threats as the threat landscape evolves. Completing the missing business case elements for these programs would provide DOD and Congress with key information to use for oversight and funding decision making aimed at delivering these critical capabilities.

The Oversight Council, responsible for overseeing DOD's various PNT efforts, also faces challenges. Specifically, while the DOD approved the Oversight Council implementation plan for overseeing DOD's PNT enterprise, the council has not developed strategic objectives for DOD's alternative PNT efforts or created metrics to measure progress toward meeting those objectives. With the addition of strategic objectives and metrics, the Oversight Council meetings could face increased attention on addressing topics related to alternatives to GPS, something not currently occurring. Further, with strategic objectives and metrics, DOD could be better able to review and measure the progress of individual efforts as well as the extent to which the overall PNT Enterprise is meeting its vision and mission. In addition, such strategic objectives and metrics could allow DOD to better assess its PNT Enterprise for potential capability gaps, conduct risk analysis, develop funding scenarios, and ensure these efforts meet needed timeframes. Further, establishing strategic objectives and metrics could enable DOD and Congress to ensure sufficient support for long-term, continuous access to vital PNT data.

Recommendations for Executive Action

We are making two recommendations to components within DOD:

The Secretary of the Navy should ensure its PNT efforts have complete business cases, including that:

- The ACNS program assesses technology and schedule risk;
- The CEC program assesses its schedule risk;
- The AN/WSN-12 program completes its schedule risk assessment and documents the decision made to leverage a technology risk assessment completed on a similar program to the AN/WSN-12; and
- The effort to add alternative PNT capabilities to GPNTS finishes its requirements documentation. (Recommendation 1)

The Secretary of Defense should ensure that the PNT Oversight Council creates strategic objectives and metrics to measure progress towards those objectives for DOD's alternative PNT efforts. (Recommendation 2)

Agency Comments and Our Evaluation

We provided a draft of this report to DOD for review and comment. DOD provided written comments, which are reproduced in appendix III and summarized below. DOD also provided technical comments, which we incorporated as appropriate. In its comments, DOD partially concurred with one recommendation and concurred with the other recommendation.

DOD partially concurred with our first recommendation. In its comments, DOD agreed a thoroughly documented business case, complete with all elements, provides leaders with the best possible information to make acquisition decisions. DOD said the Navy has already made significant progress in completing or partially completing most of the business case elements. DOD agreed that completing these elements is appropriate to reduce uncertainty and risk in their respective programs. However, DOD said not every program requires every element of a business case, and current policy gives acquisition officials the flexibility to meet these business case elements through reasonable alternatives. DOD further stated their acquisition policy relieves smaller programs like GPNTS from the need to conduct a formal independent cost estimate, due to the additional time and cost to conduct the analysis. Instead, DOD said the GPNTS program met its fiduciary responsibility through a different cost estimation process. Similarly, DOD said the AN/WSN-12 program leveraged an existing technology risk assessment to inform its decisions. DOD also acknowledged its acquisition policy did not require the ACNS program to conduct formal, standalone assessments of technology risk or schedule risk. Based upon DOD's written comments and new information provided via their technical comments, we revised our business case element assessments for some of the programs and efforts in this report.

We agree with DOD that program offices can tailor their acquisition policy requirements as necessary based on the urgency and characteristics of the capability being acquired, as well as the pathway being used. We also recognize that a formal independent cost estimate may not be feasible due to the time and expense involved. However, an alternative approach is to have a cost estimating organization outside of the program office and program executive office conduct an independent cost assessment to validate the program office's assumptions and processes used in developing their cost estimate. We also agree with DOD that stand-alone, formal assessments of technology risk and schedule risk may not be necessary for smaller, less risky programs. However, we maintain the program office can conduct an evaluation of potential technology and schedule risk and document it in place of a formal, stand-alone assessment. If alternative measures, like an existing technology risk assessment from a comparable effort, are used to inform a program's technology risk, the program should document this decision. We further contend that while a program office can tailor the elements of a business case based upon the program's size and risk, program offices should ensure they complete the fundamental elements of a business case (requirements, acquisition strategy, technology risk, schedule risk, and independent cost estimates) to inform acquisition decisions. We understand that the programs are not required to complete a full business case, however by completing these steps, the program, the department, and the Congress would be better able to make more informed choices about the risks that are being borne for these important programs. Given the critical importance of these alternative PNT programs to meet DOD's requirements for accurate PNT information in GPS contested environments, we maintain that our recommendation is valid.

DOD concurred with our second recommendation and stated the PNT Executive Management Board (EMB) has developed recommended goals and objectives for the DOD PNT Enterprise as approved by the PNT Oversight Council. DOD further stated that these goals and objectives will be monitored through regular meetings at the DOD PNT Enterprise Working Groups, and their status will be reported at EMB and PNT Oversight Council meetings. Additionally, DOD said each year progress against the goals will be addressed in the PNT Oversight Council's annual report to Congress.

We are sending copies of this report to the appropriate congressional committees and the Secretary of Defense. In addition, the report is available at no charge on the GAO website at https://www.gao.gov

If you or your staff have any questions about this report, please contact Brian Bothwell at (202) 512-6888 or BothwellB@gao.gov, or Jon Ludwigson at (202) 512-4841 or LudwigsonJ@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff members who made key contributions to this report are listed in appendix IV.

Bri Bothwell

Brian Bothwell
Director, Science, Technology Assessment, and Analytics

Jon Ludwig

Jon Ludwigson
Director, Contracting and National Security Acquisitions

Appendix I: Objectives, Scope, and Methodology

The Senate Armed Services Committee asked us to review Department of Defense's (DOD) alternative Positioning, Navigation, and Timing (PNT) efforts. This report examines: (1) the threats to PNT that DOD identified, (2) the efforts in DOD's alternative PNT acquisition and development portfolios, and if those efforts have a sound business case, and (3) how DOD is overseeing those efforts.

This report is a public version of a sensitive report that we issued on April 6, 2022.[1] DOD deemed some of the information in our April 2022 report to be sensitive, which must be protected from public disclosure. Therefore, this report omits sensitive details about seven of the 11 alternative PNT technology and product development efforts we identified. Although the information provided in this report is more limited, the report addresses the same objectives as the sensitive report and uses the same methodology.

To identify the threats to the Global Positioning System (GPS), we reviewed documents, both publicly available and from DOD. Examples of publicly available documents include the Defense Intelligence Agency Challenges to Security in Space 2019 report, the National Air and Space Intelligence Center 2018 Competing in Space report, and the Center for Strategic and International Studies Space Threat Assessments from 2019, 2020, and 2021. We identified these studies as part of our background research using internet searches. We used relevant terms, such as threats to GPS, to identify reports and studies relevant to our engagement. We also interviewed DOD officials, such as the office of DOD's Chief Information Officer. We received both unclassified and classified threat briefings from DOD's Joint Navigation Warfare Center. While we reviewed classified information, we only included information from publicly released documentation in order to report out at an unclassified level. We also scoped this objective to threats that may impact DOD's use of PNT, as we did not look specifically at civilian use of PNT.

[1] GAO, *GPS ALTERNATIVES: DOD Is Developing Navigation Systems But Is Not Measuring Overall Progress*, GAO 22-104609SU (Washington, D.C.: Apr. 6, 2022).

We took several steps to identify the alternative PNT efforts in DOD's portfolio. First, we analyzed publicly available DOD budget documentation to identify alternative PNT efforts. Next, we compared that information to a list of efforts from the PNT Oversight Council. We corroborated our list of efforts with interviews with the DOD, such as the Army Cross Functional Team. Our scope was limited to new PNT efforts or programs specifically enhancing their alternative PNT capability. We also only considered efforts in advanced component development or acquisition.[2] We did not include legacy equipment or platform upgrades that may include PNT but are not for the purpose of enhancing PNT resiliency. The intent of our methodology was to cover the major alternative PNT efforts within DOD. We identified 11 efforts on the basis of this analysis.

To gather information on each of the efforts, we sent a questionnaire to each of the 11 offices identified as leading the alternative PNT effort. We sent the questionnaire to the 11 offices in May 2021 and updated the information provided through January 2022. The questionnaire included questions about business case documentation, budget, and timelines. Of the 11 offices that we contacted, all 11 responded to our questionnaire. We followed up with interviews or a written question set as needed. Funding numbers are presented in millions of base-year 2022 dollars.

Using the completed questionnaire, along with documentation and interviews, we assessed the alternative PNT efforts against sound business case criteria. The criteria for a sound business case include:

- requirement documentation,
- an acquisition strategy
- assessment of technical risk,
- assessment of schedule risk, and
- an independent cost estimate.

We applied these criteria to identified efforts in acquisition. We evaluated if the effort had the business case element or not, based either on documentation evidence or from an interview with the DOD officials. We did not evaluate the content or quality of the business case element. We made this assessment as of January 2022.

[2] We determined the effort stage by looking at efforts with a budget activity code of 6.4 (advanced component development and prototypes) or above.

To assess how DOD is overseeing PNT, we used DOD documentation and interviews to better understand the oversight structure. Specifically, we interviewed several officials who are involved with the PNT Oversight Council, such as the office of DOD's Chief Information Officer. We also looked at the oversight structure of the military services, and interviewed the Army and Air Force PNT Cross Functional Teams, and the Navy offices responsible for alternative PNT.

We also analyzed the content on meeting minutes for the PNT Oversight Council. We reviewed the minutes from the highest level of the council from June 2020-August 2021. We omitted one meeting as the contents of the meeting were classified as Top Secret. For each meeting, there were between two and four agenda topics. The meeting minutes contain a summary of the discussion. However, the meeting minutes did not have information on the time spent on agenda topics, or exact quotes from the meetings.

Two independent analysts developed content analysis categories to characterize the range of issues that agenda topics covered, and compared categories to develop a final list. The analysts coded each agenda topic into one or more of the following five categories:

- Schedule
- Funding
- Fielding
- Procurement
- Platform status

The analysts then reviewed the meeting minutes and for each agenda topic, deciding if each agenda topic related to GPS, alternative PNT, both, or neither. For example, a discussion on GPS M-code schedule would be categorized as "GPS schedule". A discussion of Alternative PNT needing increased funding would be categorized as "Alternative PNT funding". With these categories we were able to draw conclusions on the overall content of the meeting minutes. The two analysts who conducted the content analysis discussed the discrepancies in their coding and reached agreement on them or resolved them through a third-analyst review. The final analysis produced an inventory of PNT Oversight Council topics.

Finally, we assessed DOD's oversight against portfolio criteria. We used portfolio leading practices developed by the Project Management

Institute.[3] We determined the criteria was current and could be applied to our analysis. In addition to our analysis, we confirmed in interviews with DOD that DOD officials consider PNT as a portfolio and that the PNT Oversight Council is responsible for the PNT portfolio.

We conducted this performance audit from November 2020 to April 2022 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We subsequently worked with DOD from April 2022 to August 2022 to prepare this public version of a sensitive report. This public version was also prepared in accordance with these standards.

[3] Project Management Institute, Inc., *The Standard for Portfolio Management*, 4th ed. (2017).

Appendix II: PNT Program or Effort Assessments

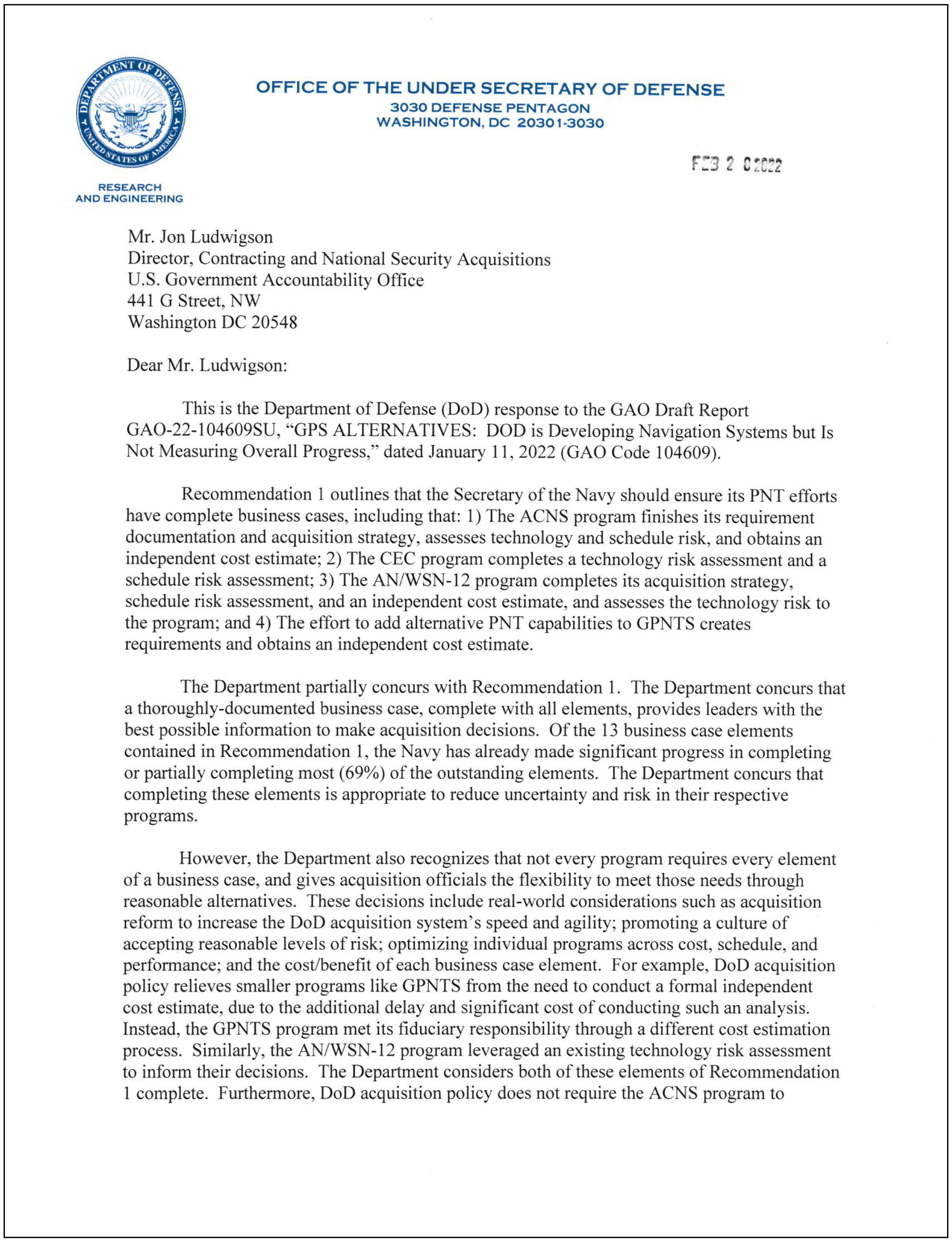
This section contains four assessments of individual Department of Defense (DOD) alternative Position, Navigation, and Timing (PNT) efforts, specifically the multi-PNT receiver efforts, we identified. Each assessment presents an overview of the effort, and information on the effort's funding, business case documentation, contracting information, technology approach, and schedule milestones.

We collected this information via questionnaires GAO sent to each military service. For all assessments, we obtained the information presented from program office responses to the questionnaire and program office documents and communication with program officials. As a result, DOD is the source of the information regarding the identity of the contractors. We did not review individual contract documents to verify information. If an effort had multiple contracts, we included the contract with the highest dollar value in the assessment.

The technology approach section categorizes technologies by relative PNT, absolute PNT, or communicate PNT. Relative PNT technologies use onboard sensors to track the position of a platform and keep time without the use of an external signal. Absolute PNT technologies use external sources of information, other than the Global Positioning System (GPS), to determine the position of a platform, geo-referenced to Earth. Communicate PNT technologies provide PNT information to various military platforms.

Funding numbers are presented in millions of base-year 2022 dollars. Information is current as of January 2022. When a standard section of the assessment page is not applicable to an effort, N/A will appear.

Appendix III: Comments from the Department of Defense



RESEARCH
AND ENGINEERING

OFFICE OF THE UNDER SECRETARY OF DEFENSE
3030 DEFENSE PENTAGON
WASHINGTON, DC 20301-3030

FEB 2 0 2022

Mr. Jon Ludwigson
Director, Contracting and National Security Acquisitions
U.S. Government Accountability Office
441 G Street, NW
Washington DC 20548

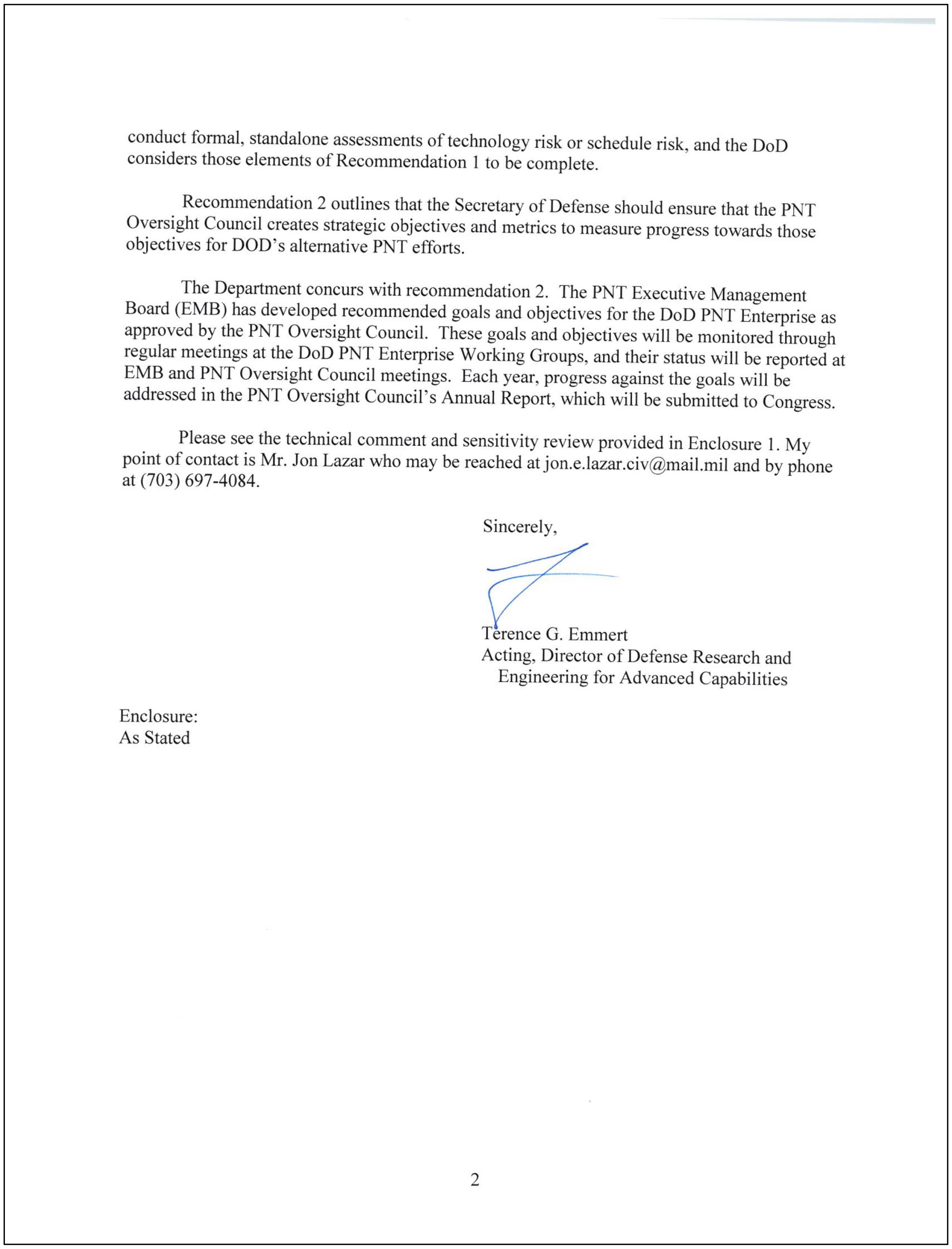
Dear Mr. Ludwigson:

This is the Department of Defense (DoD) response to the GAO Draft Report GAO-22-104609SU, "GPS ALTERNATIVES: DOD is Developing Navigation Systems but Is Not Measuring Overall Progress," dated January 11, 2022 (GAO Code 104609).

Recommendation 1 outlines that the Secretary of the Navy should ensure its PNT efforts have complete business cases, including that: 1) The ACNS program finishes its requirement documentation and acquisition strategy, assesses technology and schedule risk, and obtains an independent cost estimate; 2) The CEC program completes a technology risk assessment and a schedule risk assessment; 3) The AN/WSN-12 program completes its acquisition strategy, schedule risk assessment, and an independent cost estimate, and assesses the technology risk to the program; and 4) The effort to add alternative PNT capabilities to GPNTS creates requirements and obtains an independent cost estimate.

The Department partially concurs with Recommendation 1. The Department concurs that a thoroughly-documented business case, complete with all elements, provides leaders with the best possible information to make acquisition decisions. Of the 13 business case elements contained in Recommendation 1, the Navy has already made significant progress in completing or partially completing most (69%) of the outstanding elements. The Department concurs that completing these elements is appropriate to reduce uncertainty and risk in their respective programs.

However, the Department also recognizes that not every program requires every element of a business case, and gives acquisition officials the flexibility to meet those needs through reasonable alternatives. These decisions include real-world considerations such as acquisition reform to increase the DoD acquisition system's speed and agility; promoting a culture of accepting reasonable levels of risk; optimizing individual programs across cost, schedule, and performance; and the cost/benefit of each business case element. For example, DoD acquisition policy relieves smaller programs like GPNTS from the need to conduct a formal independent cost estimate, due to the additional delay and significant cost of conducting such an analysis. Instead, the GPNTS program met its fiduciary responsibility through a different cost estimation process. Similarly, the AN/WSN-12 program leveraged an existing technology risk assessment to inform their decisions. The Department considers both of these elements of Recommendation 1 complete. Furthermore, DoD acquisition policy does not require the ACNS program to



conduct formal, standalone assessments of technology risk or schedule risk, and the DoD considers those elements of Recommendation 1 to be complete.

Recommendation 2 outlines that the Secretary of Defense should ensure that the PNT Oversight Council creates strategic objectives and metrics to measure progress towards those objectives for DOD's alternative PNT efforts.

The Department concurs with recommendation 2. The PNT Executive Management Board (EMB) has developed recommended goals and objectives for the DoD PNT Enterprise as approved by the PNT Oversight Council. These goals and objectives will be monitored through regular meetings at the DoD PNT Enterprise Working Groups, and their status will be reported at EMB and PNT Oversight Council meetings. Each year, progress against the goals will be addressed in the PNT Oversight Council's Annual Report, which will be submitted to Congress.

Please see the technical comment and sensitivity review provided in Enclosure 1. My point of contact is Mr. Jon Lazar who may be reached at jon.e.lazar.civ@mail.mil and by phone at (703) 697-4084.

Sincerely,

Terence G. Emmert
Acting, Director of Defense Research and
Engineering for Advanced Capabilities

Enclosure:
As Stated

Accessible Text for Appendix III: Comments from the Department of Defense

FEB 28 2022

Mr. Jon Ludwigson
Director, Contracting and National Security Acquisitions
U.S. Government Accountability Office
441 G Street, NW
Washington DC 20548

Dear Mr. Ludwigson:

This is the Department of Defense (DoD) response to the GAO Draft Report GAO-22-104609SU, "GPS ALTERNATIVES: DOD is Developing Navigation Systems but Is Not Measuring Overall Progress," dated January 11, 2022 (GAO Code 104609).

Recommendation 1 outlines that the Secretary of the Navy should ensure its PNT efforts have complete business cases, including that: 1) The ACNS program finishes its requirement documentation and acquisition strategy, assesses technology and schedule risk, and obtains an independent cost estimate; 2) The CEC program completes a technology risk assessment and a schedule risk assessment; 3) The AN/WSN-12 program completes its acquisition strategy, schedule risk assessment, and an independent cost estimate, and assesses the technology risk to the program; and 4) The effort to add alternative PNT capabilities to GPNTS creates requirements and obtains an independent cost estimate.

The Department partially concurs with Recommendation 1. The Department concurs that a thoroughly-documented business case, complete with all elements, provides leaders with the best possible information to make acquisition decisions. Of the 13 business case elements contained in Recommendation 1, the Navy has already made significant progress in completing or partially completing most (69%) of the outstanding elements. The Department concurs that completing these elements is appropriate to reduce uncertainty and risk in their respective programs.

However, the Department also recognizes that not every program requires every element of a business case, and gives acquisition officials the flexibility to meet those needs through reasonable alternatives. These decisions include real-world considerations such as acquisition reform to increase the DoD acquisition system's speed and agility; promoting a culture of accepting reasonable levels of risk; optimizing individual programs across cost, schedule, and performance; and the cost/benefit of each business case element. For example, DoD acquisition policy relieves smaller programs like GPNTS from the need to conduct a formal independent cost estimate, due to the additional delay and significant cost of conducting such an analysis. Instead, the GPNTS program met its fiduciary responsibility through a different cost estimation process. Similarly, the AN/WSN-12 program leveraged an existing technology risk assessment to inform their decisions. The Department considers both of these elements of Recommendation 1 complete. Furthermore, DoD acquisition policy does not require the ACNS program to conduct formal, standalone assessments of technology risk or schedule risk, and the DoD considers those elements of Recommendation 1 to be complete.

Recommendation 2 outlines that the Secretary of Defense should ensure that the PNT Oversight Council creates strategic objectives and metrics to measure progress towards those objectives for DOD's alternative PNT efforts.

The Department concurs with recommendation 2. The PNT Executive Management Board (EMB) has developed recommended goals and objectives for the DoD PNT Enterprise as approved by the PNT Oversight Council. These goals and objectives will be monitored through regular meetings at the DoD PNT Enterprise Working Groups, and their status will be reported at EMB and PNT Oversight Council meetings. Each year, progress against the goals will be addressed in the PNT Oversight Council's Annual Report, which will be submitted to Congress.

Please see the technical comment and sensitivity review provided in Enclosure 1. My point of contact is Mr. Jon Lazar who may be reached at jon.e.lazar.civ@mail.mil and by phone at (703) 697-4084.

Sincerely,

Terence G. Emmert
Acting, Director of Defense Research and Engineering for Advanced Capabilities

Enclosure:
As Stated

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contacts

Brian Bothwell at (202) 512-6888 or BothwellB@gao.gov

Jon Ludwigson at (202) 512-4841 or LudwigsonJ@gao.gov

Staff Acknowledgments

In addition to the contacts named above, J. Andrew Walker (Assistant Director), R. Scott Fletcher (Assistant Director), Jenn Beddor (Analyst-in-Charge), Kerry Burgott, Jean Lee, and Jay Tallon made key contributions to this report. Pete Anderson, Vinayak Balasubramanian, Breanne Cave, Matthew T. Crosby, Keith McDaniel, Joslyn McKlveen, Sean Seales, and Robin Wilson also contributed to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or
TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548