NATIONAL SCIENCE AND TECHNOLOGY COUNCIL

NATIONAL RESEARCH AND DEVELOPMENT PLAN FOR POSITIONING, NAVIGATION, AND TIMING RESILIENCE

A Report by the

Position, Navigation, and Timing Research and Development Interagency Working Group

Subcommittee on Resilience Science and Technology

Committee on Homeland and National Security

August 2021

About the National Science and Technology Council

The National Science and Technology Council (NSTC) is the principal means by which the Executive Branch coordinates science and technology policy across the diverse entities that make up the Federal research and development enterprise. A primary objective of the NSTC is to ensure science and technology policy decisions and programs are consistent with the President's stated goals. The NSTC prepares research and development strategies that are coordinated across Federal agencies aimed at accomplishing multiple national goals. The work of the NSTC is organized under committees that oversee subcommittees and working groups focused on different aspects of science and technology. More information is available at http://www.whitehouse.gov/ostp/nstc.

About the Office of Science and Technology Policy

The Office of Science and Technology Policy (OSTP) was established by the National Science and Technology Policy, Organization, and Priorities Act of 1976 to provide the President and others within the Executive Office of the President with advice on the scientific, engineering, and technological aspects of the economy, national security, homeland security, health, foreign relations, the environment, and the technological recovery and use of resources, among other topics. OSTP leads interagency science and technology policy coordination efforts, assists the Office of Management and Budget with an annual review and analysis of Federal research and development in budgets, and serves as a source of scientific and technological analysis and judgment for the President with respect to major policies, plans, and programs of the Federal Government. More information is available at http://www.whitehouse.gov/ostp.

About the Positioning, Navigation, and Timing Research and Development Interagency Working Group

The Positioning, Navigation, and Timing Research and Development (PNTRAD) Interagency Working Group (IWG) is organized under the Subcommittee for Resilience Science and Technology, which is part of the NSTC Committee on Homeland and National Security. The IWG seeks to coordinate the activities of executive departments and agencies to improve the resilience of the PNT enterprise including critical infrastructure that is dependent on PNT services.

About this Document

This document was developed by the PNTRAD IWG to address requirements of Executive Order 13905 on *Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services* (February 12, 2020). It presents a national plan of research and development to improve the resilience of positioning, navigation, and timing services and the critical infrastructure that depends on such services. This document will be reviewed and updated as appropriate.[1]

Copyright Information

[1] Executive Order 13905 § 4(h) - "Once the plan is published, the Director of OSTP shall coordinate updates to the plan every 4 years, or as appropriate."

NATIONAL SCIENCE & TECHNOLOGY COUNCIL

Chair

Dr. Eric Lander, Director

Staff

Grace Diana, Acting Executive Director

COMMITTEE ON HOMELAND AND NATIONAL SECURITY

Co-Chairs

Kathryn Coulter Mitchell, Under Secretary (Acting) for Science & Technology, DHS

Jih-Fen Lei, Acting Principal Deputy, Director of Defense Research & Engineering for Research & Technology, DOD

Aaron Miles, Principal Assistant Director for National Security and International Affairs, OSTP

SUBCOMMITTEE ON RESILIENCE SCIENCE & TECHNOLOGY

Co-Chairs

David Alexander, Senior Science Advisor – Resilience, Science & Technology Directorate, DHS

Mary Erickson, Deputy Director of the National Weather Service, NOAA

Grace Diana, Interim Co-Chair, OSTP

Tracie Lattimore, Interim Co-Chair, OSTP

POSITIONING, NAVIGATION, AND TIMING RESEARCH & DEVELOPMENT INTERAGENCY WORKING GROUP

Chair

Barry Herman, Assistant Director for National Security and Emergency Preparedness, OSTP

Members

Department of Commerce

Department of Defense

Department of Energy

Department of Homeland Security

Department of the Interior

Department of Transportation

National Aeronautics and Space Administration

National Security Council staff

Office of Management and Budget

Table of Contents

Abbreviations and Acronyms

DHS	Department of Homeland Security
DOC	Department of Commerce
DOD	Department of Defense
DOE	Department of Energy
DOI	Department of the Interior
DOT	Department of Transportation
EO	Executive Order
GPS	Global Positioning System
GNSS	Global Navigation Satellite System
IMU	Inertial Measurement Unit
IWG	Interagency Working Group
M&S	Modeling and Simulation
NAS	National Airspace System
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NSTC	National Science and Technology Council
OSTP	Office of Science and Technology Policy
PNT	Positioning, Navigation, and Timing
PNTRAD	Positioning, Navigation, and Timing Research and Development
R&D	Research and Development
RF	Radiofrequency
RFI	Request for Information
SBAS	Satellite-based augmentation system
SOO	Signals of Opportunity
UTC	Coordinated Universal Time

Introduction

Positioning, Navigation, and Timing (PNT) refers to capabilities that allow for the determination of location (positioning), the ability to traverse to a new location along a path (navigation), and the knowledge of the current time (timing), all with a high level of precision. The Global Positioning System (GPS) is the premier global provider of PNT service, but any system, network, or capability that provides a reference to calculate or augment the calculation of one or more of these components is considered a PNT service. PNT use has expanded dramatically over the past few decades, becoming a largely invisible utility underpinning numerous technologies, systems, and services including those utilized for critical infrastructure functions. A corresponding growth in both intentional and unintentional disruptions, including jamming and spoofing of GPS signals places U.S. infrastructure at an elevated risk. Wide-scale interruption and manipulation of GPS could cause cascading, disrupting effects to infrastructure that would impact a large proportion of the population and threaten economic activity and national security.

Many PNT services are available with varying levels of performance (accuracy, availability, continuity, coverage, and integrity) based on a range of technological approaches and techniques. These include satellite and terrestrial radionavigation systems, specialty radars, light detection and ranging (LIDAR), wireless and fiber optic networks, vison aided navigation combined with detailed terrain maps, and local atomic clocks.

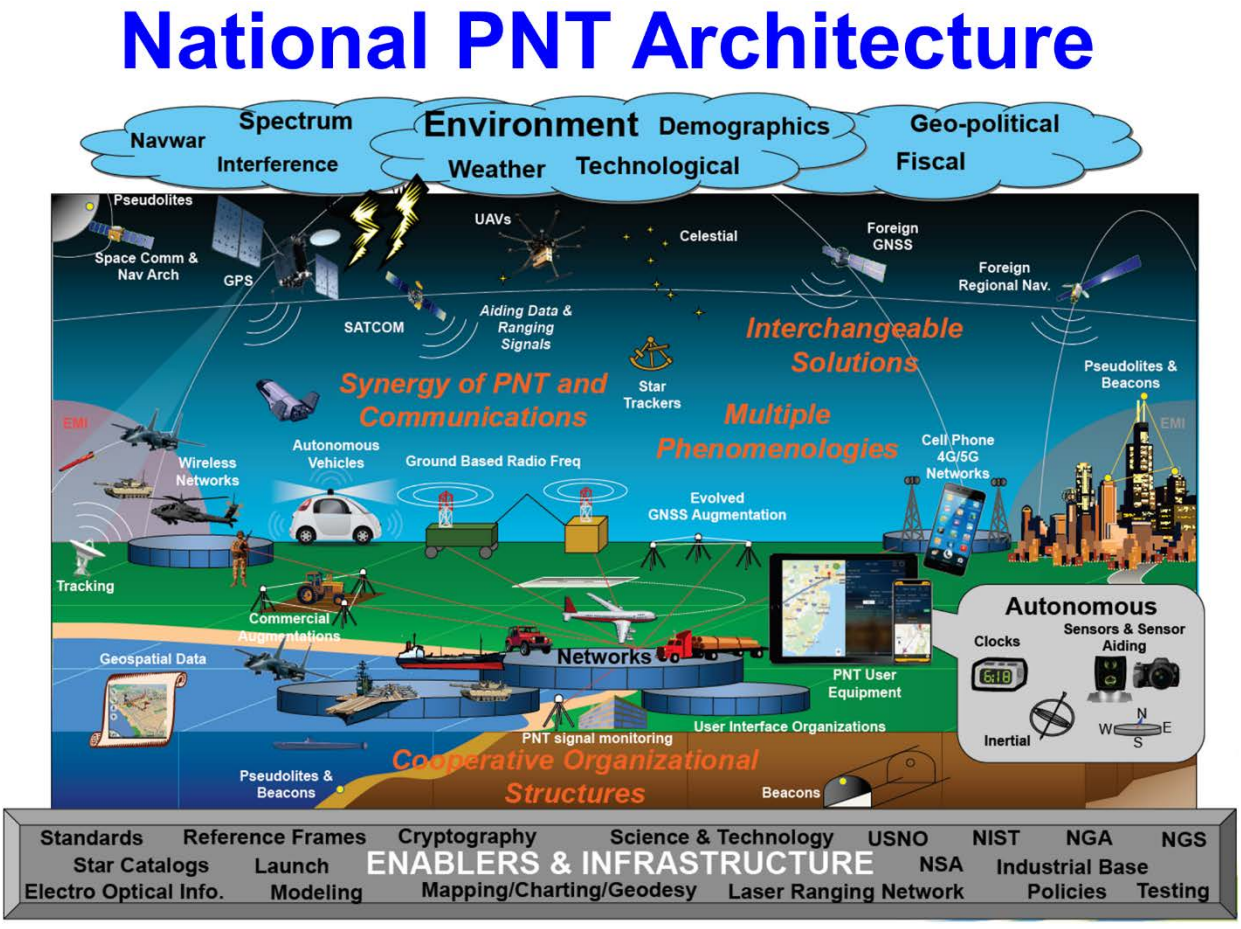

Figure 1. The National PNT Architecture shows the wide sources and applications of PNT, beyond merely satellites and user equipment. Credit DOT.

Global navigation satellite systems (GNSS) are the primary source of PNT services around the world. Currently, GPS (United States), Galileo (European Union), GLONASS (Russia), and BeiDou (China) provide global coverage while QZSS (Japan) and NAVIC (India) offer regional PNT support. Typically, autonomous, ground- or space-based systems augment these signals to improve their performance for more demanding applications (e.g., aviation and survey).[2] GNSS receiver equipment receive and refine these signals to provide geodetic infrastructure that underpins the accurate positioning within the National Spatial Reference System.[3] The geodetic infrastructure and its products, notably the terrestrial reference frame, provides the information needed to pinpoint the locations of satellite, aircraft, and ground-based instruments and the geophysical phenomena they are tracking.

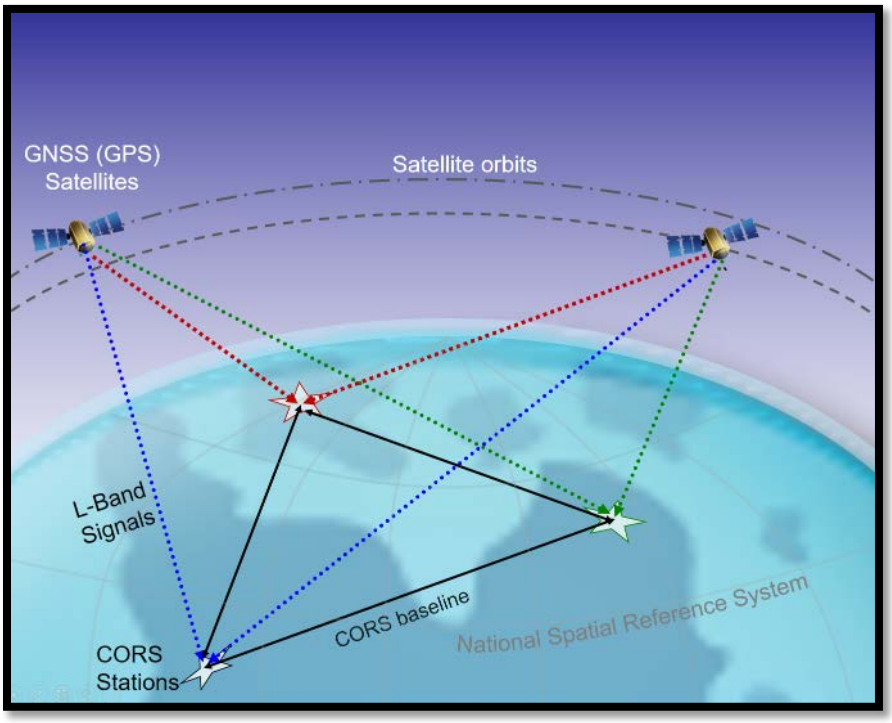

Figure 2. Shown are three Continuously Operating Reference Stations (CORS) on the ground (white stars) receiving L-Band[4] radio signals from two GNSS satellites. Over a long period of time, the positions of the CORS are resolved precisely in the National Spatial Reference System (NSRS). In turn, these positions can be used to derive improved orbits and resolve onboard clock errors for the GNSS satellites. This mutually supportive relationship establishes precision and accuracy for positioning in the NSRS. It is predictable and reliable and will highlight disruptions in the L-Band signal. Credit NOAA.

The U.S. Government sustains support of GPS providing a global PNT service that is open, stable, accurate, and free to access. This has resulted in the incorporation of PNT data and capabilities into numerous applications, systems, services, and infrastructure sectors. Beyond the familiar use of mapping and navigation functions, PNT systems, "have become a largely invisible utility for technology and infrastructure, including the electrical power grid, communications infrastructure and mobile

[2] Figure 1 in this document provides a visual example of the mutual relationship between satellites and ground stations in GNSS.

[3] More information about the Geodetic Infrastructure required may be found in "Evolving the Geodetic Infrastructure to Meet New Scientific Needs", National Academies of Sciences, Engineering, and Medicine (2020), https://doi.org/10.17226/25579.

[4] Designated by the Institute of Electrical and Electronics Engineers as covering the 1-2 GHz RF band.

devices, all modes of transportation, banking and finance, precision agriculture, weather forecasting, and emergency response."[5] Additionally, PNT services increase the efficiency and productivity of construction and mining; enable the precise time transfer required for communication networks and financial markets; enable scientific pursuits such as improvements to earthquake monitoring; improve satellite orbit determination and aid space situational and space domain awareness efforts; improve the accuracy of oil and natural gas pipeline in-line-inspection equipment; support the rapidly-increasing Internet of Things (IoT); enable autonomous and semi-autonomous vehicles; and help protect national security by improving the logistics and operational effectiveness of the military.

Naturally-occurring interference, unintentional sources of man-made interference, and intentional jamming and spoofing can disrupt the weak GNSS-based PNT signals resulting from the thousands of miles between the satellite transmitter and the terrestrial receiver (see Box 1). Signal interference (data or measurement) can result in degradation or complete loss of PNT service. Similarly, signal spoofing by an attacker can result in loss of application performance causing erroneous PNT results that may lead to altered functioning of systems or altered decision making, usually in the attacker's favor (See Box 2). The onset of these effects can be instantaneous or delayed and it is possible for effects to continue even after the spoofing has ended.

Many critical systems depend solely on GNSS for PNT service and have not been designed or tested to effectively respond to its disruption and manipulation. This places those systems, which are used in multiple sectors of U.S. critical infrastructure,[6] at an elevated risk. Disruption and manipulation of PNT services could compromise national security, increase the risk of loss of life, severely impact the economy, and disrupt the daily activities of the American people. The compound risk posed when interference or loss of PNT services happens simultaneously with other disasters, natural or man-made, escalates impacts and has the potential to seriously impede mitigation and recovery.

Various legislative and Executive policy directives seek to lower the risk from a potential PNT service disruption. Space Policy Directive 7 on The United States Space-Based Positioning, Navigation, and Timing Policy[7] established overall policy for improving GPS performance and resilience. The National Defense Authorization Act of 2018[8] and the National Timing Resilience and Security Act of 2018[9] authorized funding for certain resilience enhancements such as the development and demonstration of backup GPS capabilities. Executive Order (EO) 13905, *Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services* (February 2020)[10] directed a comprehensive approach that utilizes risk management to improve the resilience of critical infrastructure that is dependent on PNT service. The EO further directs the development of a national plan for the research and development (R&D) and pilot testing of additional resilient PNT services that

[5] Executive Order 13905, Strengthening National Resilience through Responsible Use of Position, Navigation, and Timing Services, 12 February 2020.

[6] Presidential Policy Directive 21 (PPD-21), titled *Critical Infrastructure Security and Resilience*, identifies 16 critical infrastructure sectors that are so vital to the United States that their incapacity or destruction would have a debilitating effect on national security, the economy, public health or safety, or any combination thereof.

[7] https://www.whitehouse.gov/presidential-actions/memorandum-space-policy-directive-7

[8] https://www.congress.gov/bill/115th-congress/house-bill/2810

[9] Included in the Frank LoBiondo Coast Guard Authorization Act of 2018, https://www.congress.gov/bill/115th-congress/senate-bill/140

[10] https://www.federalregister.gov/documents/2020/02/18/2020-03337/strengthening-national-resilience-through-responsible-use-of-positioning-navigation-and-timing

are not dependent on GNSS, with the stipulation that the plan include approaches for integrating and using multiple PNT services.

The National PNT Architecture Study of 2008 (National PNT Architecture) describes capabilities needed to meet the anticipated future requirements of a resilient PNT enterprise with expanded applications and users. As noted in the National PNT Architecture, GPS has been and will continue to be the foundation of U.S. PNT services. Improvements to resilience that address both GPS and other PNT sources will be most effective in satisfying the larger strategic objectives of preserving national, homeland, and economic security. A resilient PNT enterprise is one that includes the use of multiple, diverse sources of PNT and data paths, the choice of architectures that minimize attack opportunities and overlapping attack vectors that could reduce protections or result in single points of failure, the utilization of defense-in-depth (multiple layers of protections, mitigations, and responses), and the integration of modern cybersecurity principles into the greater PNT enterprise, among other key resilience-improving capabilities. Other needs in the PNT enterprise include the ability to deliver and use PNT in physically or electronically impeded environments, to consistently provide higher accuracy with greater assurance, to provide notification of degraded or misleading information, to provide PNT services at high altitudes and in space, and to develop adequate modeling and simulation capabilities, including capabilities to predict how PNT services are affected in urban environments.

Box 1: Jamming and Spoofing

The PNT signals received from GNSS are exceptionally low power compared to other radio signals. This makes it easy to interfere with GNSS receivers. Interference arises from intentionally and unintentionally produced RF waveforms that overwhelm the satellite signal, thus degrading or denying a receiver's ability to operate. Deliberate interference is categorized as jamming or spoofing.

Jamming is the production of signals that have the same effect as interference; the only difference is the intent to degrade or deny a target receiver's operation.

Spoofing, also known as manipulation, is the creation of signals that mimic true signals in some ways, but deny, degrade, disrupt, or deceive a receiver's operation when they are processed. Spoofing may be unintentional, such as effects from the signal of a GNSS repeater, or they may be intentional and even malicious.

- Measurement spoofing introduces signals that cause the target receiver to produce incorrect measurements of time of arrival or frequency of arrival or their rates of change.
- Data spoofing introduces incorrect digital data to the target receiver for its use in processing of signals and the calculation of PNT.

Either type of spoofing can cause a range of effects, from incorrect outputs of PNT to receiver malfunction. The onset of these effects can be instantaneous or delayed and it is possible for effects to continue even after the spoofing has ended.[11]

Resilient PNT receivers will be better able to identify and operate through jamming and spoofing attempts, switch to additional PNT sources that are not experiencing interference, provide PNT solutions for longer periods of time without receiving updates from trusted PNT services (holdover), and avoid unacceptable degradation in performance.

[11] Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure, DHS, https://www.us-cert.gov/sites/default/files/documents/Improving_the_Operation_and_Development_of_Global_Positioning_System_%28GPS%29_Equipment_Used_by_Critical_Infrastructure_S508C.pdf

National R&D Plan

This national plan for research and development (R&D) to promote critical infrastructure resilience against disruptions in PNT services, was developed pursuant to EO 13905 and within the broader context of improving overall U.S. PNT resilience and the geodetic infrastructure required to support it. This R&D plan can help fulfill the capability needs identified above and is consistent with the broader vision and strategy of the National PNT Architecture. Since GPS is the premier provider of global PNT, R&D activities towards improving the capabilities and resilience of its augmentations and its users' receivers are a natural and important component of implementing the strategy. However, both the National PNT Architecture strategy and the EO recognize that GPS alone cannot meet the requirements of all users, including the desire for overall PNT resilience. Additional PNT services and systems that are not reliant on GPS (or, more generally, GNSS), with vulnerabilities and failure modes that are sufficiently dissimilar to those of GNSS, must be developed or improved to meet these needs. This plan's goal is to inspire the conception of fundamentally new approaches to resilient PNT technologies and services.

The R&D plan supports three overarching goals for greater PNT[12] service resilience, including GPS resilience and the development of additional PNT capabilities and services,[13] and prioritizes fourteen R&D objectives for further R&D across these overarching goals:

Characterize and Model PNT services and their use

- Characterize PNT system requirements
- Improve test capabilities and test protocols for assessing equipment and services
- Conduct modeling, simulation, and testing to assess vulnerabilities
- Develop tools to identify appropriate sources of PNT service based on functional requirements

Improve and Expand PNT capabilities

- Improve PNT holdover capabilities
- Develop and improve external sources of additional PNT services
- Establish calibration and traceability techniques
- Improve and expand disruption detection tools and mitigation methods
- Prototype and demonstrate new PNT services

Integrate and Deploy resilient PNT

- Determine concepts and techniques for securely integrating multiple sources of PNT service
- Common hardware platforms
- Develop resilient PNT system architectures
- Investigate operating internal sources as primary sources of PNT service
- Develop cybersecurity standards, best practices, and other guidance

Each objective includes a description of R&D that will help advance the respective goal, and a recommendation regarding which departments and agencies (agencies) should consider supporting R&D in the given area. Agencies should prioritize among these R&D objective areas, as appropriate, through regular budgeting and planning processes, informed by continuing interagency discussion and coordination. Agencies should further coordinate these R&D activities with State, local, Tribal, and Territorial

[12] Unless otherwise specified, in this document, PNT refers to the totality of the PNT ecosystem, including data, services, information, and infrastructure. PNT includes GPS, other GNSS, and complimentary PNT systems and services.

[13] Additional PNT capabilities and services are those technologies that provide PNT information other than GPS. They can augment, back-up, replace or verify GPS in host applications.

governments, foreign governments and organizations, academia, and private industry. Such coordination should provide additional opportunities to leverage resources and capabilities to increase the resilience of the PNT enterprise and better ensure our national, homeland, and economic security.

Box 2: Dependence on PNT and Impacts to Critical Infrastructure

PNTservices are essential for the safe operation of our nation's critical infrastructure. PNT services are used across many critical infrastructure sectors and enable vital operational aspects of transportation, communications, energy distribution, and emergency response operations. For some applications, PNT disruptions may be limited to reduced operational efficiency. For other applications, impacts may range from loss of service, such as interruptions to power delivery, to jeopardy for safety-of-life operations such as aviation or autonomous vehicles.

An outage in one critical infrastructure sector has the potential to create cascading consequences in other sectors. For example, spoofing of PNT clocks in the power grid could cause power outages and impact other sectors enabled by the electricity subsector. Disruption of the communication sector by PNT jamming or spoofing could lead to failures in emergency services, financial, and information technology sectors. A cigarette-lighter GPS jammer on a shipping truck parked near an airport could lead to air traffic control and navigation problems cascading to transportation, industrial and emergency services sectors. Current, publicly available devices can cause a ship to navigate off its intended course or disable high-speed communications by desynchronizing equipment.

Goal I. Characterize and Model PNT services and their use

Agencies should characterize and model current and future PNT system and service capabilities, performance characteristics, vulnerabilities, and the projected future needs of PNT users. Many users of PNT, including those in the critical infrastructure sectors, may not fully realize the extent of their dependence on PNT services nor the full risk of potential cascading effects on their operations posed by disruptions in service. Determining effective resilience measures first requires a comprehensive understanding of these system vulnerabilities and the interconnections and interdependencies between systems. Similarly, developing new or improved PNT services requires an understanding of the evolving technical needs of PNT applications. This section identifies four critical R&D objectives that support a better understanding of the vulnerabilities of PNT services and systems, as well as the capabilities and needs of the PNT enterprise. This section also focuses on improving and using modeling and simulation tools and test capabilities that can inform the development of resilience-enhancing technologies and techniques.

1.1 Characterize PNT system requirements

Agencies should characterize PNT system requirements to ensure the performance, safety, and reliability of PNT services for applications under various operating conditions relevant for that system. Varied mission needs include operations in urban canyons, underground, in space, in varying geographic regions (global and/or regional), in the transition from sea to shore in littoral regions, and in electromagnetically-impeded conditions.

Agencies should define these mission requirements to aid the identification of additional PNT services required for each use case.[14]

Agencies should also support research that characterizes the PNT performance requirements for these operations coupled with additional PNT services in the presence of GNSS and without GNSS. [DHS, NOAA, USGS, DOT, NASA]

1.2 Improve test capabilities and test protocols for assessing equipment and services

Agencies should improve and expand their test facilities and capabilities, as needed, to support assessments of vulnerabilities in user equipment and additional PNT technologies, to allow verification of new technologies and techniques including resilience enhancements, and to mimic actual user environments and use case scenarios. This research should include human factors impacting PNT service effectiveness.

Agencies should support R&D to develop the programs and protocols needed to ensure the safety, calibration and robustness of PNT equipment and services. The implementation of testing capabilities and protocols for individual, commercial, and government PNT users and developers should utilize different approaches depending on the risk level of the application and the sophistication of the equipment.

Agencies should support development and dissemination of test vectors to aid in the self-assessment of equipment vulnerabilities. Agencies should support R&D for testing of PNT technologies including a range of operating conditions and edge cases. Agencies should support identifying, monitoring, and

[14] These services may include inertial reference units, local oscillators, fiber timing services, ground- and space-based RF services, and visual systems that can meet the needs of user populations.

testing industry innovations that improve the integrity and availability of PNT data for transportation and other critical sectors. [NOAA, USGS, DOT, NASA]

1.3 Conduct modeling, simulation, and testing to assess vulnerabilities

Agencies should support additional research to develop models, simulations, and tests to determine how PNT outages impact essential services and applications, and to develop strategies to mitigate adverse consequences. Critical scenarios for further investigation include understanding the effects of timing service disruptions on the power, communications, and financial sectors; the effects of jamming and spoofing interference on maritime navigation, and the effects of GNSS disruptions to aircraft systems, positive train control, connected/autonomous vehicles, and NAS infrastructure. Where practicable, the results of computational analyses should be validated through hardware testing.

Agencies should support continuing efforts to further enhance the live-sky testing environment and to conduct vulnerability testing of critical infrastructure and commercial equipment (both fixed and mobile assets) to uncover vulnerabilities to natural and artificial interference and to manipulation of GPS and PNT augmentation signals.

Agencies should support R&D analyzing PNT equipment and systems to assess vulnerabilities and attack vectors in advance of their widespread adoption. Finally, agencies should support R&D of tests to assess the performance of GNSS, GNSS augmentations, and additional PNT services to identify sources of errors, including human factors, and determine methods for correcting them. [DHS, USGS, DOT, NASA]

1.4 Develop tools to identify appropriate sources of PNT service based on functional requirements

Agencies should support research to develop tools that can assess performance of PNT equipment and services individually and as integrated systems within a wide range of constraints and operating conditions. These tools should analyze advanced threats and evaluate the impact of performance changes in PNT on mission effectiveness. Agencies should support R&D to develop the capability to simulate a variety of constraints on GPS availability and accuracy to enable the evaluation of a wide combination of candidate PNT technologies. These tools should also simulate the impacts of different levels of GPS availability and integrity scenarios to help evaluate and find acceptable combinations of additional PNT sources to maintain mission performance. [USGS, DOT, NASA]

Goal II. Improve and Expand PNT capabilities

Agencies should work to improve and expand PNT services and capabilities across the enterprise by developing PNT equipment with better performance specifications (e.g., accuracy, availability, continuity, coverage, and integrity) to enable greater resilience, as well as innovations (e.g., size, weight, power consumption, and cost) to motivate its adoption. New applications that use PNT information, and the desire to improve existing applications, will demand more stringent technical requirements from PNT services. Conversely, improvements in PNT capabilities will drive the development of new applications and the enhancement of existing ones. This push-pull effect in the development cycle should result in iterative and continuous improvements across the PNT enterprise. By enhancing calibration and traceability techniques combined with detecting and mitigating interference, PNT assurance may be obtained. The following five resilience improving R&D objectives span the concept, development, and operational phases.

2.1 Improve PNT holdover capabilities

A system that relies on PNT information can operate on its own for a period of time without access to external PNT services if it has its own internal capabilities that replicate PNT signals with, for example, clocks and inertial measurement units (IMUs). This capability is termed “holdover”. However, systems holdover capabilities drift from the true measurement – both in position and time measurements - eventually exceeding the acceptable error limit for the application. The time required to exceed the error limit can range from seconds to months, depending on the specific system and application. Simultaneously, the rate at which error accumulates can vary based on the physical environment of the equipment. Extending holdover times could be an effective mitigation during times of PNT disruption, enabling system architectures with reduced dependence on external PNT sources, which would reduce vulnerability in user equipment.

Agencies should support research to improve the performance of these internal sources of PNT while simultaneously decreasing their size, weight, power use, and cost to satisfy the requirements of the widest possible set of users. Specific technologies to focus on in the short-term include accelerometers, gyroscopes, gravity field modeling, and clocks. In the long-term, quantum sensing can lead to breakthroughs. Agencies should support research in portable optical lattice and chip-scale atomic clocks with longer mean time between failures, along with new time and frequency transfer methods consistent with optical clock performance. Agencies should support R&D for timing holdover including local networks of clocks to increase stability, direct links between clocks to the NIST optical clock infrastructure, and determining elevation by relativistic time differences. Agencies should also support research to improve holdover capabilities by developing vertical control and gravity field models to extend the length of time IMUs can operate independently. [NIST, NOAA, USGS, DOT, NASA]

2.2 Develop and improve external sources of additional PNT services

Agencies should support research to develop and improve additional PNT sources so that they can be evaluated and deployed as part of a resilient next-generation PNT architecture. Research in sources of additional PNT should include a diverse range of characteristics, including: local, regional, and global coverage, with additional considerations for Low Earth Orbit constellations; cislunar[15] coverage and

[15] In this document, Cislunar refers to the region of space beyond Geosynchronous Orbit, or GEO, (approximately 36,000 km above sea level) and through Lunar Orbit (approximately 385,000 km from Earth), where navigation

applications; relative and absolute PNT information; failure modes; and bands on the electromagnetic spectrum. These sources, and their corresponding services, should be evaluated for application to a variety of use cases, from deep space exploration to fixed-location terrestrial critical infrastructure equipment, as appropriate.

Agencies should support R&D into emerging PNT needs. An emerging need will be in the growth of the space industry for on-orbit, cislunar PNT services for which there are fewer options, because most PNT services are directed towards the Earth. Agencies should support position signal research for deep space including specific technologies related to low-frequency, long-range signals. Agencies should support R&D into Synthetic Aperture Radar (SAR) as well as Interferometric SAR (InSAR) to monitor infrastructure positions and update for motion. Agencies should also support R&D for distributing timing signals including but not limited to time dissemination over fiber-optic networks that extend to distant locations with a requisite time precision, ground-based navigation systems including pseudolites, and distributed atomic clocks.

Agencies should support research in alternative relative navigation methods that leverage the natural environment for PNT information. These include but are not limited to vision-aided and terrain-based navigation on land, magnetic and gravitational field mapping in the air, nautical charting and bathymetry at sea, and X-ray and optical sources in space.

In addition to developing and deploying PNT systems, agencies should support research on how existing signals can be used to support PNT resilience. Signals of opportunity (SOO) and other existing signals, such as WWVB[16], can be used to verify PNT signals or approximate PNT information if a PNT service is disrupted or denied. SOO can also be used to distribute frequency for relative timing applications or provide timing through common view approaches. Agencies should support research to understand how SOOs such as AM and FM radio signals, broadcast TV, and cellular base-station signals can promote PNT diversity without widescale infrastructure investment. [DHS, NIST, NOAA, USGS, DOT, NASA]

2.3 Establish calibration and traceability techniques

Calibration and traceability are crucial to maintaining the performance specifications of PNT systems. Agencies should support research to develop and validate PNT service calibration methods and geodetic infrastructure to establish traceability and quality systems for a wide range of end users. Specific goals should include modeling of GNSS satellite orbits and a network of ground monitoring stations to establish fiduciary control as a means of calibration, while simultaneously providing improved traceability to address jamming, spoofing or other interference. Agencies should support R&D for calibration methods and traceability within industries such as the financial sector, which is required to ensure metrological traceability to Coordinated Universal Time (UTC). Agencies should also support other areas of research including the development of antenna calibration methods for GNSS signals

is typically performed through ground-based tracking and analysis of two-way communication signals to and from the spacecraft . Users in this region can also opt to use GPS and other observables for on-board real-time orbit/trajectory determination . For context, the GPS Terrestrial Service Volume (TSV) spans between Earth's surface and 3000 km altitude (Low Earth Orbit), and the GPS Space Service Volume (SSV) from 3000 km altitude to GEO .

[16] WWVB is a NIST-operated radio station located near Boulder, Colorado that distributes low-precision time and frequency to the continental US and other parts of North America. https://www.nist.gov/time-distribution/radio-station-wwvb

and augmentations to reduce reliance on adversarial entities and better maintain calibration standards. [NIST, NOAA, USGS]

2.4 Improve and expand disruption detection tools and mitigation methods

Interference detection and mitigation (IDM) capabilities are critical to resilient PNT architectures. Agencies should support R&D for various methods and tools to aid in IDM on both system-level and end-user PNT devices, including methods to automatically detect adjacent band emission and in-band interference and mitigation methods from PNT disruptions and interference. This includes sensors that can detect signal power anomalies and correlations that would indicate a spoofing attempt, an anti-spoofing toolkit that includes detectors that span the full radio frequency processing chain, and other various jamming and spoofing detection and measurement tools and techniques.

Agencies should also pursue R&D in antenna-based mitigation and detection methods for PNT interference, including beamforming/nulling, for different form factor civilian antennas, including patch antennas for embedded devices. Agencies should support R&D and testing for software defined radios (SDR), sensors, to include directional antennas, and software for highly automated systems. Agencies should support research to develop methods to reduce latency in recognition and reporting of interference, jamming, and spoofing. Agencies should support further development of algorithms for verifying and integrating multi-PNT sources capable of performing IDM to uncover accuracy issues. Agencies should also support R&D of simulation tools to aid in the development of such resilient next-generation PNT architectures.

Agencies should support further research to create an IDM monitoring system that integrates real-time, large-scale monitoring of receiver signals in critical infrastructure and reports results to a centralized data processing system for enterprise trending and data mining. This system would allow greater collaboration between agencies and industry to analyze and share trends, develop timely joint interdiction responses and provide notification to the public as appropriate, continually improve PNT technologies, and identify emergency response actions for major disruptions. Agencies should support other research in artificial intelligence and machine learning to help identify discontinuities and disruptions to PNT sources, such as the Continuously Operating Reference Stations (CORS) network, which can alert analysts to GPS interference and other natural disruptions like earthquakes. Agencies should support research in sensor fusion of timing sources to help detect manipulation and erroneous signals from sudden offsets and subtle drifts. [DHS, NOAA, DOT, NASA]

2.5 Prototype and demonstrate new PNT services

Agencies should support R&D, pilot testing, and demonstrations for additional PNT service (such as those discussed in Objective 2.2) deployment and validation. Agencies should also support pilot testing programs for additional PNT services that may improve positioning accuracy in urban canyons, such as vehicle-to-everything-based position correction systems. [DHS, NIST, DOT, NASA]

Goal III. Integrate and Deploy resilient PNT

Agencies should integrate and deploy resilient PNT architectures through development of prototype systems and demonstrations. PNT resilience comes not only from improving and expanding capabilities for PNT services, anomaly detection, and holdover technologies; just as important is how these capabilities and components are integrated into user equipment. Design and architecture principles are applied within a PNT solution for a given application in an absolute reference frame and, where appropriate, in a relative reference frame (navigation or time). Resilience throughout the PNT enterprise is further promoted through the development and use of standards and best practices. Developing standards and other guidance also expands the availability and adoption of resilient PNT by disseminating useful information to designers and manufacturers and promoting uniformity and commonality in PNT approaches, architectures, and interfaces. The five R&D objectives identified below advance these aspects of the overall plan.

3.1 Determine concepts and techniques for securely integrating multiple sources of PNT service

Standard filtering algorithms can integrate multiple sources of PNT signals. However, agencies should support additional research to develop techniques to do this integration securely, efficiently, and with integrity. Agencies should support R&D in next-generation resilient PNT receivers that employ a modular architecture allowing plug-and-play capability for incorporating multiple sources of PNT (both internal and external) through standard common interfaces that pass not just PNT data, but also quality metrics from each source, as appropriate, to the system. These quality metrics should help inform a system's resilient PNT fusion algorithm, while taking into account that the metrics themselves may be erroneous or spoofed.

In order to leverage PNT data through multiple sources, agencies should support R&D in resilient fusion algorithms that can leverage various quality metrics for each source, infer various degrees of trust and integrity to those signals over time, and produce a mixed-source solution with higher reliability than the individual PNT signals. An absolute or geometric frame of reference is a set of coordinates that can be used to determine positions, velocities, and trajectories of objects in that frame; while a relative reference frame is where different frames of reference move relative to one another. A relative reference frame can complement geometric frameworks to increase PNT resilience, and agencies should support additional research to enable potential resilience benefits. Additionally, agencies should support R&D to investigate relative timing between applications and/or between multiple applications.

Agencies should support research to analyze signal integrity from different PNT sources to identify outlier signals and to isolate compromised signals so they do not corrupt other receiver functions. Agencies should also support research to determine which combinations of PNT sources should be integrated to provide PNT solutions and to understand what conditions should result in a user switching to a different combination.

Additionally, as PNT systems begin to incorporate more PNT sources, it is important to recognize each additional PNT source as a new potential vulnerability. Agencies should support multiple-source integration R&D in PNT systems and the associated design mitigations required to prevent the introduction of new vulnerabilities.

Finally, agencies should support research to design, prototype, test, and validate the authentication algorithms and receivers and update PNT system standards based on these results. [DHS, NIST, DOT, NASA]

3.2 Common hardware platforms

As the next generation of PNT systems incorporate more PNT sources, agencies should support research for integrating multiple PNT sources onto common hardware platforms to reduce size, weight, power, and cost (SWaP-C) factors in user equipment. Otherwise having separate hardware and antennas for each PNT source may become impediments to adoption of PNT source diversity in user systems. Agencies should support research in software-defined radios as one possible pathway to accomplish this. Agencies should support R&D for architecture designs that could integrate beamforming/nulling antennas for increased resilience to interference and spoofing. Common hardware platforms can also be vulnerable to common mode failures, so agencies should support R&D in user equipment standards to ensure they include appropriate requirements for hardware diversity.[17] [DHS, DOT, NASA]

3.3 Develop resilient PNT system architectures

Due to expanded PNT capabilities including new PNT services, better disruption detection tools, and improved holdover devices are important for PNT resilience, agencies should support R&D for the next generation of PNT user equipment and how to integrate these components and design system architectures in ways that are resilient and robust. Agencies should support research on how receiver system architectures can, when efficacious, be redesigned to reduce their dependencies on external sources and improve their ability to continue operating securely even in the presence of PNT source corruption and disruption. This approach should also include incorporating cybersecurity and resilience principles from the Resilient PNT Conformance Framework.

This framework and other standards should promote safety in automated systems, especially in automated transport. Agencies should support the development of tools and technologies that integrate and coordinate cyberspace capabilities to ensure the integrity of PNT information. Agencies should support additional research to assess the feasibility of a federated timing network of regional clocks that are periodically updated to UTC and to develop new time and frequency transfer methods that are consistent with optical clock performance. [DHS, NIST, USGS, DOT, NASA]

3.4 Investigate operating internal sources as primary sources of PNT service

Resilience of systems can be improved by strictly controlling external access to the system which limits the opportunities for attack and interference. One method to limit access is by utilizing internal sources as the primary PNT solution. External access is blocked completely until the system needs to verify its PNT data and correct for any drift that may have occurred by referencing an external PNT source, which should be done at randomized intervals. Agencies should support research to explore which applications and at what holdover thresholds this would be beneficial to systems and systems-of-systems. Agencies should support research in systems that monitor additional PNT signals other than GNSS for positioning/navigation. Agencies should support the development of demonstration tests and prototype systems to verify the efficacy of the approach. [DHS, NIST, NOAA, DOT, NASA]

[17] Common mode failures are those that occur when two or more systems fail in the same way for the same reason. They may occur at different times because of design differences or repeated external events. NASA, https://ntrs.nasa.gov/citations/20160005837

3.5 Develop cybersecurity standards, best practices, and other guidance

In addition to hardware and software development, agencies should support research to develop improved understanding of the resilience and vulnerability of PNT constituents to develop and publish improved cyber and physical security standards, best practices, and other guidance for industry and PNT users. Agencies should funnel the research outcomes of the previous sections of this plan into these efforts. Agencies should support R&D, testing, and validation of new and additional PNT services for compliance with new and existing cybersecurity standards. To achieve sustained and resilient PNT services, agencies should also remain engaged with Federal stakeholder agencies responsible for spectrum governance and regulatory policies and on how the current National spectrum governance and regulatory policies affect PNT operations. Agencies should support development of a conformance framework for defining resilient PNT equipment that can operate with improved resilience within these governance structures.

Agencies should support the development of best practices documents to codify the use of software and hardware assurance and additional sources of PNT. Agencies should support the development and adoption of cybersecurity principles through partnerships with academia and industry. Agencies should support the development and promulgation of training objectives and standards to all relevant groups, including trade/technical schools. Agencies should support the development of guidance documents and GPS interface control documents for user equipment that define when, how, and what services to use for PNT data synchronization. Agencies should also support the development of other standards including authentication algorithms for satellite-based augmentation systems (SBAS) aviation receivers, which can be used as a model for more comprehensive use of signal and data authentication protocols.

Agencies should support research to ensure the availability of testing and validation platforms to ensure compliance with cybersecurity standards, and best practices, as well as enabling spectrum system certification, and Federal licensing. These research efforts may be guided by the NIST PNT Profile, and incorporated into updates of existing cybersecurity standards and best practices like the NIST Cybersecurity Framework, which have been developed and adopted through partnerships with industry, academia, and government.[18, 19] [DHS, NIST, USGS, DOT, NASA]

[18] https://www.nist.gov/pnt

[19] https://www.nist.gov/cyberframework currently version 1.1

Interagency and Non-Federal Coordination and Alignment

Implementing this R&D plan requires a whole-of-government effort. Many agencies are involved in sustaining and advancing U.S. PNT capabilities through active R&D programs. Some agencies have developed a tremendous knowledge base and extensive technical capabilities through decades of research effort. Leveraging these resources across government within a collaborative framework can provide greater efficiencies in R&D activities and help avoid unnecessary duplication. The National Space-Based PNT Executive Committee will participate in the interagency coordination process, collaborating with agencies across government to help avoid duplication of previous GPS-related resilience research.

Table I summarizes the recommendations in this plan regarding agencies that should consider supporting and contributing to specific R&D objectives.

Organizations outside of the Federal Government are also essential to improving critical infrastructure resilience against disruptions to PNT service. State, local, Tribal, and Territorial governments have direct control over certain types of infrastructure and, more generally, have interest in preserving the operational capabilities of the infrastructure that is located within their jurisdictions.

Additionally, most U.S. infrastructure is owned or operated by private sector entities, and many sources of additional PNT have been developed and deployed as commercial assets. There is a growing recognition within the private sector that resilience improvements are necessary[20] and that cooperation and collaboration with the government is advantageous to realizing this common goal. This collaboration should include sharing appropriate test data to understand PNT threats and how to mitigate them, organizing industry days, hosting competitions, and facilitating data exchange for interface development. Agencies should support and leverage cooperative research and development agreements (CRADAs) and other technology transfer mechanisms to partner with industry.

University research groups are one of the primary means through which the Federal government supports fundamental research activities. Universities also provide a pipeline of educated and trained scientists and engineers to maintain the workforce required by the PNT enterprise.

Finally, many foreign governments and organizations are interested in improving the PNT resilience of their own infrastructure. Coordination with these entities not only improves the resilience of infrastructure around the world and provides additional avenues of international cooperation, but can also help ensure U.S. national security activities broaden the R&D enterprise and expand the PNT resilience knowledge base at a faster rate. Agencies should collaborate with these organizations and leverage outside capabilities and resources to strengthen the PNT enterprise.

[20] National Space-Based Positioning, Navigation, and Timing Advisory Board Topic Paper (September 2018); https://www.gps.gov/governance/advisory/recommendations/2018-09-topic-papers.pdf

Table I: Recommendations regarding agency support for R&D objectives

		DHS	DOC/NIST	DOC/NOAA	DOI/USGS	DOT	NASA
Characterize and Model	Characterize PNT system requirements	●		●	●	●	●
	Improve test capabilities and test protocols for assessing equipment and services			●	●	●	●
	Conduct modeling, simulation, and testing to assess vulnerabilities	●			●	●	●
	Develop tools to identify appropriate sources of PNT service based on functional requirements				●	●	●
Improve and Expand	Improve PNT holdover capabilities		●	●	●	●	●
	Develop and improve external sources of additional PNT services	●	●	●	●	●	●
	Establish calibration and traceability techniques		●	●	●		
	Improve and expand disruption detection tools and mitigation methods	●		●		●	●
	Prototype and demonstrate new PNT services	●	●			●	●
Integrate and Deploy	Determine concepts and techniques for securely integrating multiple sources of PNT service	●	●			●	●
	Common hardware platforms	●				●	●
	Develop resilient PNT system architectures	●	●		●	●	●
	Investigate operating internal sources as primary sources of PNT service	●	●	●		●	●
	Develop cybersecurity standards, best practices, and other guidance	●	●		●	●	●

Conclusion

Implementing this R&D plan will advance resilience and efficiency across the PNT enterprise in a coordinated and cost-effective, manner. Federal agencies should continue to assess their evolving PNT requirements and R&D needs. This plan will be reviewed at least every four years and updated as needed to reflect any significant changes determined through periodic assessments. Future updates should continue to align new R&D activities to agency responsibilities, and identify areas of mutual interest, facilitate collaboration, avoid duplication, and leverage investments for maximum benefit.

Coordination with entities outside of the Federal Government will allow additional opportunities for leveraging resources effectively toward greater national resilience to ensure our national, homeland, and economic security.