Complementary PNT Action Plan

DOT Actions to Drive CPNT Adoption

U.S. Department of Transportation
John A. Volpe National Transportation Systems Center
55 Broadway
Cambridge, MA 02142-1093

617-494-2000
www.volpe.dot.gov

September 2023

Contents

1. Objective

The U.S. Department of Transportation (DOT) is the lead for civil positioning, navigation, and timing (PNT) requirements in the United States and represents the Federal civil departments and agencies in the development, acquisition, management, and operations of the Global Positioning System (GPS). The Office of Positioning, Navigation, and Timing and Spectrum Management (within the Office of the Assistant Secretary for Research and Technology) coordinates the development of Departmental positions on PNT and spectrum policy to ensure safety, mobility, and efficiency of the transportation network. The Department also provides civil PNT system policy analysis and coordination representing Federal civil agencies responsible for critical infrastructure in the requirements development, acquisition, management, and operations of GPS.

These efforts support Federal policy governing PNT programs and activities for national and homeland security, civil, commercial, and scientific purposes. These include Executive Order 13905, *Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Service*s (EO 13905), and Space Policy Directive 7, *The United States Space-Based Positioning, Navigation, and Timing Policy* (SPD-7). These policies are directed towards PNT users and U.S. Federal space-based PNT service providers, respectively.

The primary and most recognizable PNT service supporting critical infrastructure is GPS. However, because GPS relies on signals broadcast from satellites in medium Earth orbit (MEO), signal strength at the receiver is low and thus vulnerable to intentional and unintentional disruptions. In 2020, the U.S. Department of Transportation (DOT) Volpe National Transportation Systems Center (Volpe Center) conducted field demonstrations of candidate PNT technologies that could offer complementary service in the event of GPS disruptions. The purpose of the demonstrations was to gather information on PNT technologies at a high technology readiness level (TRL) that can work in the absence of GPS. The Volpe Center, through a competitive acquisition process, selected 11 candidate technologies to demonstrate positioning or timing functions:

- Two vendors demonstrated low Earth orbit satellite PNT technologies—one L-band and one S-band;
- Two vendors demonstrated fiber-optic timing systems, both based on the White Rabbit Precision Time Protocol (PTP);
- One vendor demonstrated localized database map matching database, inertial measurement unit (IMU), and ultra-wideband (UWB) technologies; and,
- Six vendors demonstrated terrestrial radiofrequency (RF) PNT technologies across low frequency (LF), medium frequency (MF), ultra-high frequency (UHF), and Wi-Fi/802.11 spectrum bands.

Five of the technologies were demonstrated at Joint Base Cape Cod (JBCC) and six were demonstrated at NASA Langley Research Center (LaRC). The demonstrations were scenario-based implementations consisting of a series of scenarios modeled on critical infrastructure use cases under various operating

conditions. PNT technology vendors were encouraged to participate in all timing and positioning scenarios that they deemed to be compatible with the capability of their technology at the time of the demonstration. While this demonstration was a snapshot in time, there were two central recommendations from the demonstration:

1. U.S. DOT should develop system requirements for PNT functions that support safety-critical services.
2. U.S. DOT should develop standards, test procedures, and monitoring capabilities to ensure that PNT services, and the equipage that utilize them, meet the necessary levels of safety and resilience identified in Recommendation 1.

The culmination of the demonstration program was the 2021 Report to Congress, Complementary PNT and GPS Backup Technologies Demonstration Report (2021 Demonstration Report). The PNT resiliency recommendations distilled in the 2021 Demonstration Report were vetted through a Federal interagency review process. During the same period, SPD-7 (directed to U.S. Federal Space-Based PNT service providers) and EO 13905 (directed to PNT users) were issued in a coordinated effort to strengthen U.S. PNT policy.

As part of its ongoing responsibilities as civil PNT lead, the Department has developed this Complementary PNT Action Plan to drive CPNT adoption across the Nation's transportation system and within other critical infrastructure sectors. The plan describes actions that the DOT will pursue over the next several years, including engaging PNT stakeholders; monitoring and supporting the development of CPNT specifications and standards; establishing resources and procedures for CPNT testing and evaluation; and creating a Federal PNT Services Clearinghouse. Taken together with efforts of other Federal partners, these initiatives will continue to strengthen the resilience of the Nation's PNT-dependent systems, resulting in safer, more secure critical infrastructure.

2. Actions to Drive Adoption

This Action Plan establishes five broad lines of effort that DOT will pursue to implement this CPNT Action Plan.

1. Stakeholder engagement,
2. Specifications and standards development,
3. Field trial and test range development,
4. Establish a Federal PNT Services Clearinghouse, and
5. Domain-specific CPNT Services acquisition support.

2.1 Stakeholder Engagement

The Department, in its capacity as the civil lead for PNT, is focused on recent efforts to strengthen the resilience of safety-critical PNT systems, within the transportation sector and across all critical infrastructure sectors. A core strategy to accomplish this objective is stakeholder engagement. DOT serves on or supports several Federal bodies, such as the National PNT Executive Committee and the National Space-Based PNT Advisory Board.

In August 2022, the Department held a CPNT Roundtable as an in-person/virtual event at DOT Headquarters in Washington, DC. Stakeholders were invited from across the PNT enterprise, which included both providers of PNT services and critical infrastructure owners and operators that have identified dependence on PNT. The goal of the roundtable was to discuss opportunities and challenges with regard to adoption of suitable and mature PNT technologies so that users are assured that they will have the resilient PNT services they need to operate safely during any disruption, denial, or manipulation of GPS service. The CPNT Roundtable identified several key takeaways:

From PNT Technology Vendors

- GPS has had excellent reliability
- GPS represents a market anomaly created by the impression that it is a free service/utility
- Cost is a concern for adoption of other PNT technologies
- CPNT technologies must provide increased capability, not viewed only a backup to GPS
- There is a need for “sandbox” facilities, test ranges, and pilot programs for soft entry to mature operations
- CPNT technologies need to have a mature threat posture against capable actors
- CPNT must be viewed as a system-of-systems approach with layered/overlapping services
- There is a need for Federal PNT contract language and for the Federal Government to lead as an investor/subscriber of services
- Standards and requirements serve a role to promote innovation and adoption

From Critical Infrastructure Consumers of PNT

- The Federal Government must demonstrate a commitment to resilience through procurement of CPNT services
- Cost and technology risk are decision factors for CPNT vs. GPS in fixed infrastructure

Based on these key takeaways, the Department committed to developing this CPNT Action Plan, the objective of which is to strengthen the safety, security, and economic health of U.S. critical infrastructure. This outcome can be achieved through adoption of CPNT services that improve the resilience of PNT functions those systems depend upon. The U.S. Government's purchasing power can also drive adoption. To do so successfully, it must be done with deliberate and informed actions. The DOT CPNT Action Plan expresses a three-fold strategy to achieve the resiliency objective set out by this policy combination:

1. Raise standards on PNT services to a level suitable for safety critical application
2. Establish field trial testing, monitoring, and situational awareness capability that is suitable for assessing PNT performance to fulfill the sandbox need
3. Drive Complementary PNT adoption through government purchasing power of PNT services at the stringent levels of performance required by critical infrastructure.

2.1.1 Government as Lead Adopter

Market development of a resilient PNT environment would be accelerated through the Federal Government's leadership and purchasing power. Congress has appropriated funds to the Office of the Assistant Secretary for Research and Technology (OST-R) in Fiscal Years 2022 and 2023 suitable for early procurement of resilient PNT services that can be evaluated in more stringent settings than the 2020 Demonstration "best light" scenarios. In some early adoption cases, these PNT services may even be utilized in the context of mitigating PNT vulnerabilities as identified in the EO 13905 PNT Profile development. As Sector Risk Management Agencies (SRMAs) prioritize their PNT operational vulnerabilities through risk-based management, they can adopt suitable and effective PNT services from viable vendors to implement resilient mitigation of those risks.

The important ingredient in the CPNT marketplace is establishing and evaluating what it means to be "suitable and effective." To that end, attention is drawn back to the recommendations in the 2021 Demonstration Report. Performance against a set of requirements driven by each critical infrastructure sector benefits from the development of broad-based open standards for PNT resilience, particularly for complementary PNT services.

Standards development processes have long lead-times and are currently underway in several forums. As described in Section 2.2, one of the elements in this Action Plan is to track and, where appropriate, provide input to those standards bodies. However, to accelerate the complementary PNT service adoption objective, the CPNT Team will undertake pathfinder efforts with critical infrastructure operators and CPNT vendors who have identified near-term needs and solutions.

2.2 Specifications and Standards Development

The transportation sector has some of the most stringent performance requirements in terms of accuracy, integrity, continuity, availability, and reliability for PNT services. Consequently, developing system requirements that focus on safety and resilience will allow determination of which requirements

are currently met, and which requirements may require further commercial innovation. DOT also supports open safety standards to promote private-sector innovation and commercial product development.

An important step to improving PNT resilience is to raise the bar by assembling a CPNT standards framework rather than the demonstration framework used in 2020. This framework transformation will be achieved by harmonizing EO 13905 directed products based on the NISTIR 8323 PNT Profile and PNT contract language, as well as applying the Protect, Toughen, Augment, and Adopt (PTAA) principle strategy. More precisely, the application specific requirements are synthesized from existing and evolving standards as well as using relevant scenario specifications where standards are lacking.

2.2.1 Specifications

The diversity and evolution of transportation and critical infrastructure applications result in varied levels and types of specifications. PNT performance needs and constraints driving the choice and applicability of a complementary PNT solution are different for aviation, rail, maritime, and on-road vehicles. Some of these constraints include environmental conditions, relevant dynamic variables and their required safety bounds, path predictability stipulating the geographic deployment configuration of a PNT complementary service, and standards and design constraints governing particular mode and use-case within a mode of transportation.

Strengths and vulnerabilities of existing complementary PNT sources can vary based on the specific application and operating environment. For example, a vessel in an open ocean marine environment operates under open sky conditions along the majority of a voyage, which makes satellite-based PNT systems (e.g., GPS or GNSS) less prone to multipath induced errors. Under those conditions, an operator could tolerate relatively large position errors (10s of meters). However, a complementary PNT solution using ground transmitter signals must be able to operate at very large distances from transmitters if it is to be effective for the marine environment.

On the other hand, human operated or automated ground vehicles operate in varied and challenging environments where sky visibility is poor in highly urbanized environments and require significantly tight requirements on position. However, they can be in proximity to transmitters for ground transmitter-based solutions. Furthermore, on-board remote sensors can be used to self-localize effectively acting as a CPNT solution.

Due to such varied PNT constraints and needs, a tractable approach is to develop PNT specifications, as well as to choose the type of CPNT solutions for evaluation and adoption based on mode, use-case, and/or scenario. This work will leverage existing operational experience and standards where available and work towards developing specifications as part of an evaluation framework where lacking. These specifications will prioritize safety but will also aim for CPNT solution(s) that improve operational efficiency. In the end, the goal is to assess the use-case relevant specifications as part of an evaluation framework during vendor field trials.

2.2.2 Resiliency Standards

A large body of work has arisen from the awareness of vulnerabilities in PNT functions that are invoked by everyday devices, which range from convenience items to operational controls for critical infrastructure that keeps the country running. Trusted standards bodies from transportation, communications, and energy sectors have begun to harmonize and refine the literature on methods, metrics, and standards for specifying PNT resilience.

The CPNT Team will participate in standards development bodies relevant to PNT resiliency enhancements. The scope includes standardization efforts focused on the definition of application-specific PNT requirements for transportation and other critical infrastructure, as well as PNT systems performance and resiliency requirements. Part of informing and supporting such standards work includes producing publications on resiliency requirements and empirical assessments of system performances under nominal and threat conditions relevant to target applications. The key government as well as industry driven standards considered include:

- National Institute of Standards and Technology (NIST), via NISTIR 8323 and the EO 13905 directives;
- Institute of Electrical and Electronics Engineers (IEEE), via P1952;
- SAE (formerly the Society of Automotive Engineers) V2X Core Technical Committee;
- 3rd Generation Partnership Project (3GPP), via 5G and 6G standards;
- Defense Innovation Unit (DIU) Harmonious Rook, via standards for collecting, storing, and utilizing RF interference data;
- International Civil Aviation Authority (ICAO), International Maritime Organization (IMO), and Radio Technical Commission for Aeronautics (RTCA), via standards products relating to PNT resilience; and,
- Other bodies that take up standards development for PNT resilience.

The active participation in, and tracking of, PNT standards builds on internal departmental research, development, and testing efforts with published products (technical papers and reports) informing these standards. Past and on-going efforts supporting requirements and resiliency standards include the 2020 Demonstration analysis and results, the framework development and testing for automated vehicles PNT systems, as well as analysis and testing of live sky PNT threat scenarios. Future application-specific research efforts informing standards include intelligent transportation, connected automated vehicles, and PNT applications for unmanned aircraft systems (UAS), rail, and maritime domains.

Efforts informing resiliency standards will include implementation, evaluation, and testing of protected toughening solutions, as well as well as fusion approaches and algorithms of CPNT solutions. It will also consider a baseline for pre-fusion of individual CPNT resiliency requirements. The output results of PNT toughening development and testing of existing and open-source concepts including antenna array techniques as well as the role of fusion in resiliency is discussed later in this section. The participation and tracking of standards is expected to be a multi-year (3–5 years) level of effort, driven by the

expected nominal evolution speeds of standard development and the broad technical skills needed for a meaningful and impactful participation in that process.

2.2.2.1 PNT Toughening

The National Space-Based PNT Advisory Board has promoted three principles—protect, toughen, and augment (PTA). This Action Plan extends the PTA principles to include *adoption*, thus PTAA where adoption is motivated by the U.S. Government's role in realizing the original PTA principles. The CPNT Action Plan seeks to support that adoption. The augmentation principle is inherent in that the "complementary" aspect of CPNT services seeks to supplement existing PNT services such as GPS, other GNSSs, or even other CPNT services.

Not so obvious is the application of the toughening principle. While a direct approach to incentivizing toughened PNT solutions is technically attractive, the current political landscape makes such investment in developing CPNT technology solutions more fraught. The strategy here is to invoke all available toughening solutions on the core GPS (or GNSS) PNT service and use that resiliency performance as the lower bound for CPNT solutions to meet. The toughening of GPS/GNSS receivers in this context is equivalent to building resiliency against intentional or unintentional threats.

Resiliency to disruption involves one or more layers of defense. Approaches include antenna and front-end designs, adaptive spatiotemporal processing techniques, sensor fusion with built-in fault monitors, validation of demodulated data from received GPS signals. Toughening technologies characterization and development activities undertaken in the course of this Action Plan or other SPD-7/EO 13905 would be made available. Example of such efforts are development and implementation of fusion algorithms with fault monitors, and characterization of adaptive beamforming solutions capabilities and limitation outside of proprietary constraints.

While augmentation and toughening principles are listed separately, they are not mutually exclusive. The implementation and adoption of a CPNT solution compatible with particular application(s) is predicated on such a CPNT solution providing added benefit to using GPS or GNSS solution alone. Such benefits include allowing for a valid PNT solution meeting the application requirements during a GPS signal disruptions or during denial of service. This is discussed in more detail in Section 2.2.2.2.

As engineering efforts are undertaken in the course of this Action Plan or other SPD-7/EO 13905 activities, those efforts that lead to toughening technology development for CPNT technology, as well as for GNSS would be made available. Some examples that relate to standards and requirements development efforts are two method authentication and adaptive antennas toughening technologies, as well as leveraging the navigation solution enhancement through optimal fusion of CPNT system output solutions on the user equipment.

2.2.2.2 Sensor Fusion of Services

One area of engineering that is necessary to realize the potential enhancements offered by CPNT solution(s) is development of sensor fusion algorithms. From the perspective of system-of-systems and

layering of services, a plurality of PNT service providers offer resilience through diversity. De minimis, the diversity approach to resilience is additive mitigation. However, to achieve higher levels of resilience efficiently, the complementary solutions should be logically combined to provide to leverage the strength of each technology and detect disruptions. This is effectively performed through PNT fusion algorithm with a resiliency engine.

Benefits of a well-designed sensor fusion of CPNT and GPS solutions include enhanced integrity and continuity of operation, as well as fault detection and exclusion. While these functions of a CPNT solution do not directly improve the resiliency of a GPS receiver, they do enhance the resiliency of the PNT solution provided to the user. In order to implement successfully such toughening measures, the CPNT solution signal disruptions known fault modes must be bounded. Monitors to detect faulted conditions for the CPNT solutions (as is the case for GPS Receiver Autonomous Integrity Monitoring (RAIM)) also need to be part of the overall solution. Additionally, any common mode faults between CPNT and GPS needs to be well understood. The reason being is that such faults or threats can go undetected by the fusion-based fault monitors reducing or fully negating the benefit of using a CPNT solution.

This Action Plan places a premium on the measures of effectiveness that evaluate PNT resilience. Further, the standards framework will be designed to also separate between sensor fusion solutions that rely on provisioning the provider, the receiver, or both.

2.2.2.3 Monitoring and Situational Awareness

An important consideration in establishing a standards framework to promote CPNT adoption is the inclusion of standards—or at least drivers, or monitoring and assessment functions—that provide operational performance and situational awareness to the users of a CPNT service. The fundamental information provided by a monitoring and assessment function ensures service commitments and assists in the detection of interference to the CPNT service. The standards development framework will identify performance monitoring and situational awareness metrics that in turn support operational concepts for critical infrastructure that have a regulatory or legal requirement.

Provisioning of performance monitoring services is expected to be phased, beginning with available capabilities developed by the core Complementary PNT Testing team and maintained by the Volpe Center. As critical infrastructure partners and PNT Service vendors are informed of the performance monitoring needs and requirements of PNT Service buyers, third-party vendors (possibly cross-cooperating CPNT service vendors) will be engaged with the intent of providing contract-based Service Level Agreements for the monitoring function.

2.3 Field Trial and Test Range Development Program

The operational maturity of some PNT-dependent markets for critical infrastructure presents the need to mimic operational enterprises so that CPNT service concepts can be configured and evaluated without affecting active operations. An open question for the Federal Government is how to develop

facilities that can support the evaluation function. Three models used in the past for test and evaluation should be explored:

1. Critical infrastructure test ranges.
2. Federal Government-hosted field campaigns.
3. Vendor fielded operating regions.

The objective of all three models would be to evaluate a CPNT service against measures of effectiveness (MoEs) from a more stringent posture and in a challenged environment than that used to conduct the 2020 Demonstration. As discussed later in this document, the MoEs used as part of this action plan will be refined and enhanced beyond what was used in the 2020 demonstration so that they are suitable to evaluate a PNT services for safety and economic impacting operations. The increased level of stringency comes in the form of objective-based metrics (rather than rubric-based criteria), vulnerability-informed threat vectors, and actively denied and/or degraded scenarios. Preparing and conducting CPNT evaluations would necessarily involve members from all three segments (operators, vendors, government), regardless of which test range model is used. However, there are significant differences in the cost, time, and resource allocations between these three models.

The U.S. Government has a variety of acquisition strategies to lead and/or support evaluation initiatives, some of which are already in use. Specifically, there are several viable approaches for DOT to establish pathfinder programs that can support any of the field trial test and evaluation models:

- Small Business Innovative Research programs (SBIR)
- Operating Administration specific contracts (through the Request for Proposal (RFP) process) (contracting vehicles described in FAR Parts 16.2 through 16.6)
- Broad Agency Announcement solicitations (BAA) (FAR 35.016)
- Basic Ordering Agreements (BOA) (FAR 16.703)
- Other Transaction Authority (OTA) (49 U.S. Code § 5312)

As vendors and critical infrastructure operators are brought together through this Action Plan, the DOT CPNT Team recommends either a BAA, BOA, or OTA acquisition path to provide the flexibility necessary to facilitate buyer-to-vendor adoption of the capabilities that meet the stringent resiliency performance and diverse geographic operating requirements of critical infrastructure systems. The acquisition will include provisioning, installation, and operation of CPNT vendor services at field trial locations. Given the breadth of technologies and vendors who participated in the 2020 demonstration, the recommended approach is to prepare a BAA, BOA, or OTA for the PNT program to be issued in April 2023 with an initial “Rapid” phase starting late FY23 and lasting 12–14 months and a second “Continuity” phase that can leverage a broader range of field trial platforms and PNT services over a 14–20 month timeframe. The additional timeframe will allow for lessons learned to be included in the second phase.

The BAA and OTA models provide flexibility, signals topical intent to vendors, and can be executed in a short timeframe as compared to the other approaches. Further, the BAA and OTA is well suited to

continued and coordinated procurement in the event addition funding is appropriated in FY24 or later fiscal years. Given Congressional intent to facilitate adoption of Complementary PNT technologies as quickly as possible, DOT should choose the path that will be most expeditious.

2.3.1 Vulnerability and Performance Test Range Development

Just as DOT and other Federal agencies have been concerned about threats to GPS from jamming and spoofing and ensuring the performance of GPS can meet safety-critical performance requirements, DOT and our partners need to be concerned about vulnerabilities and performance of CPNT technologies. It is important to establish a test range capability to evaluate CPNT solutions with quantitative performance metrics, particularly regarding resilience. The implementation should be scalable for operational use at least in early adoption phases, and it should be replicable to accommodate the three test-range models described in Section 2.3.

A "light" analysis of alternatives on the three test range models will inform the path forward on implementing test range capability with specific trade-spaces on portability, time to solution, and achievable reference precision. Critical infrastructure operators and PNT vendors responding to the solicitation will be actively sought out and engaged by the CPNT Team on available or planned PNT test ranges that can be leveraged or transformed to provide the broadest set of CPNT technologies to be evaluated. In the end, the CPNT team will determine the best field trial model for each technology being tested with a focus on performance, vulnerability threat vectors, and fault monitoring capability. Location selection will factor both public and private partnerships. To the extent possible, the team will leverage a single field trial sites for multiple technologies. During the continuity phase of testing, the team will look for opportunities to leverage the existing field trial sites and test range setups with the expansion of technology users and vendors.

As an adoption accelerator, JBCC will be considered the baseline PNT vulnerability test range as it was used for the 2020 CPNT Demonstration field campaign. The JBCC facilities will be upgraded to track GPS and CPNT additions and improvements since the 2020 campaign and thereby serve to evaluate baseline capability and field trial host participants. The primary addition to the facility is installation of equipment to create a challenged or stressful PNT environment. As with any identified test range, a test range information sheet will be prepared including schematic, equipment checklist, PNT challenged environment protocol(s), and personnel roles and responsibilities.

The explicit purpose of test range upgrades described by this Action Plan is to support the evaluation of more stringent standards and vulnerability test vectors for CPNT services as described in Section 2.2.

2.3.2 Innovative Solutions to Address PNT Capabilities Shortfall – Driving Gap Fills

A parallel "Gap Fill" effort will be conducted to address challenging applications with PNT performance needs not satisfied through existing CPNT service solutions. The objective of this effort is to develop and test capabilities that drive larger scale CPNT service development, implementation, and adoption of solutions to address gaps. Primary CPNT solutions considered will leverage existing sensors and

equipage to implement and test these solutions for applications and conditions where current PNT solutions are not adequate. This will include characterizing simulated and field trial environments utilizing the established field trial and test range locations. The gap fill analysis effort will also evaluate performance enhancing and toughening technologies against GNSS and CPNT vulnerability threat space(s).

In particular this effort will focus on challenging applications requiring high-precision and resilient dynamic PNT solutions. This gap fill effort spans 3 levels of PNT technologies:

1- Toughening Solutions: Evaluate, utilize, and test GNSS toughening solutions under controlled threat conditions to investigate the effectiveness and limitations such solutions. One class of solutions include multi-element antennae with adaptive beamforming (including adaptive nulling and main beam steering) with ITAR and non-ITAR restricted implementations. These solutions capabilities and limitations can be evaluated from open literature using simulations, lab, chamber testing, and field testing as complementary evaluation methods that provide significant information on the limitation and capabilities of such solutions under various scenarios and a battery of threat vectors.

2- Complementary PNT Sources: Evaluate, enhance, and implement PNT solutions in GNSS denied or challenging environments that leverage existing sensors and augmentation information as well as consider promising solutions currently being developed and standardized by the industry. One example is the implementation, testing, and maturation of optical based absolute positioning solution with built-in integrity monitoring capabilities in GNSS degraded or denied environment for ground navigation application. Such solutions coupled with appropriate fusion and PNT sources fallback algorithms will enable the safe operations of challenging applications that are not easily supported with currently available commercial solutions.

3- Fusion Algorithms: Evaluate and utilize various PNT fusion techniques with integrity and resiliency engines in an open-source form so as to inform and accelerate adoption of such capabilities and inform standards by providing information on the potential and limitation of such fusion approaches. This information includes the fusion capability to improve resiliency and other safety related performance metrics for challenging applications.

2.3.3 Leverage PNT Profiles

The EO 13905 policy driver for PNT resilience points directly at the SRMA-provided PNT profiles as the basis of vulnerabilities to consider in developing a threat space for testing and evaluation of PNT services. The CPNT Team will amass available PNT Profiles and use that data to develop threat models that can be projected onto candidate PNT solutions as a set of test vectors when operating in field trials. The battery of test threat vectors is expected to grow rapidly and then converge over time as the basis of PNT Profiles works through any initial backlog. Situational awareness of the threat space should be maintained across the U.S. Government interagency, and in conjunction with the SRMAs to inform updates to PNT Profiles. It may also be advantageous to promote a mature battery of test threat vectors into a Cyber Test Range PNT module.

2.3.4 Stress Testing and Scenarios

Concurrent development of testing scenarios and contested environments starts with the 2020 Demonstration as a proto test range. Those early testing scenarios will be applied to the reference system and at least two preliminary PNT service levels will be documented and exercised in one or more test ranges. The 2020 Demonstration established 14 baseline MoEs, along with their respective rubrics:

1. Capability subset (MoE-1 through MoE-9). These MoEs can be evaluated using inherently more quantitative rubrics.
    - MoE-1: Technical Readiness–System (TRL 6-9)
    - MoE-2: Technical Readiness–User Equipment (TRL 6-9)
    - MoE-3: Timing and Positioning Accuracy (as residual error; meters, nanoseconds)
    - MoE-4: Spectrum Protection (protected, owned, leased, shared)
    - MoE-5: Service Deployment Effort (low, medium, high)
    - MoE-6: Service Coverage per Unit of Infrastructure (number of transmitters per unit area covered; units/km^2)
    - MoE-7: Service Synchronization (UTC, cascade, self-synchronizing)
    - MoE-8: PNT Signal Robustness (strong, weak)
    - MoE-9: Service Resilience (fail-safe, -over, -soft, -hard)
2. Suitability subset (MoE-10 through MoE-14). The MoEs in this group that can be evaluated using inherently more qualitative rubrics.
    - MoE-10: PNT Distribution Mode (terrestrial RF, orbital RF, fiber, database)
    - MoE-11: Service Interoperability (high, low)
    - MoE-12: PNT Information Security (high, medium, low)
    - MoE-13: Time to Service Implementation (short, medium, long)
    - MoE-14: PNT System/Service Longevity (long, medium, short)

A crucial effort in the development of vulnerability scenarios and testing is the refinement of the capability (quantitative) MoEs from rubrics into testable metrics. Where appropriate the suitability (qualitative) MoEs will be revised to encapsulate remaining vulnerability and performance metrics as either updated rubrics or conditional qualifying factors for CPNT service. Performance testing will include both nominal and challenged conditions. Selection of use cases for evaluation will factor in safety, economic and social implications, and leverage any existing baseline performance requirements applicable to the PNT function.

2.4 PNT Services Clearinghouse

Action 4 of the CPNT Action Plan has a goal of achieving a significant procurement vehicle for PNT service contracts that meet the needs of one or more critical infrastructure stakeholders under the elevated policy in EO 13905 and SPD-7 on resilient PNT and stakeholder regulations. The vision is to develop a CPNT marketplace for Federal users—akin to a General Services Administration (GSA) schedule of vendors—where users would find a range of vetted and qualified service providers.

2.4.1 Federal Marketplace Strategy

The Federal Government should develop a schedule of PNT services (e.g., performance, monitoring, user equipment, and contract vehicles). This Action Plan enters a procurement framework strategy through the United States Digital Service (USDS) Digital Services Playbook and, where applicable, extends the Department of Homeland Security Mobile Application Playbook (MAP) to PNT Services. The Digital IT Acquisition Professional Program (DITAP) is an existing model suitable for specialization to the PNT services domain. DOT, and specifically OST-R through the Office of PNT and Spectrum Management, will serve as the lead agency in identifying and coordinating the team for moving a CPNT Services Clearinghouse forward. Interpretation of recent congressional appropriations currently suggests this would result in the establishment of a DOT program office for [C]PNT services. This office would also include an operations center that provided real-time situational awareness, performance monitoring, and response.

2.4.2 Apply PNT Contract Language

The interagency PNT Contract Language Development Working Group has developed a PNT Contract Language Guideline that is directly applicable to the CPNT domain. The Guideline provides key actions for acquisitions personnel that leverage the NIST Foundational PNT Profile (NISTIR 8323) through the five-function Cybersecurity Framework. The Guideline contains draft language that can be tailored to specific acquisition initiatives as well as tabletop exercises to inform the acquisition process on Federal policy for improving PNT resiliency. Suitable pathfinders emerging from the "sandbox programs" for field trials that have viable vendor-buyer matches under the stakeholder engagement will serve as the motivating use case(s). The DOT CPNT Team will incorporate output products, knowledge, and experience gained by the Department's specific efforts in response to EO 13905.

2.4.3 Incentives for Vendor-based Layering and Collaboration

One of the beneficial outcomes that OST-R achieved in conducting the 2020 GPS Backup and Complementary PNT Demonstration was the structured, formal introduction of PNT service vendors to one another. The collaborative nature of the demonstration led directly to subsequent vendor partnerships to provide improved PNT service resilience as motivated by the measures of effectiveness. PNT service resilience products have both matured and expanded since that demonstration. New vendors are entering the field and, through EO 13905, critical infrastructure stakeholders have deepened their knowledge and expectations of those services. This Action Plan incentivizes additional vendor-collaborative products and services by increasing the rigor of those metrics and establishing a testing regimen that evaluates performance more stringently.

2.5 Application Domain Acquisition Support for CPNT Service

As discussed in Section 2.2.1, the performance and constraints of individual modes or applications might drive the compatibility of a particular CPNT service. Therefore, the consideration and characterization of each CPNT solutions will consider the known PNT needs and requirements for maritime, rail, and surface applications and leverage other DOT efforts developing application specific PNT performance and resiliency requirements. In a subsequent phase of the Action Plan, CPNT service options will be made

available as both performance enhancements and mitigation options for the Department's Operating Administrations (e.g., MARAD, FRA, FAA, ITS JPO) requiring improved resilience of PNT functions. For example:

- Maritime Domain – Ready Reserve Force and Strategic Sealift Fleets
- Rail Domain – Positive Train Control Operationally Challenged Regions
- Surface Domain – Vehicle Automated Driving Systems
- Aviation Domain – National Airspace (NAS) Services, Navigation Aids, Unmanned Aircraft Systems

3. Milestones and Activities

The preliminary milestones and functional activities associated with implementing this action plan are detailed below.