January 26, 2023

Public Wireless Supply Chain Innovation Fund Implementation
ref: DOC/NTIA Docket No. 221202–0260 / Regulations.gov Docket No. NTIA-2022-0003
submitted via Regulations.gov

OVERVIEW

The Open PNT Industry Alliance (OPIA) strengthens economic and national security by supporting government efforts to accelerate the implementation of positioning, navigation, and timing (PNT) capabilities for critical infrastructure. Made up of more than 20 companies, OPIA promotes the broadest possible range of technologies to meet the PNT requirements of critical infrastructure, including telecommunications. In its comments, OPIA provides information and insight about how PNT should be a prominent feature in the Public Wireless Supply Chain Innovation Fund to promote the deployment of 5G networks and ensure their security.

OPIA – ADVOCATING FOR INNOVATIVE COMMERCIAL PNT SOLUTIONS

The Open PNT Industry Alliance is a coalition of positioning, navigation, and timing (PNT) manufacturers and service providers. The coalition members are dedicated to helping their customers back up and complement GPS by delivering multiple forms of PNT. Collectively, we advocate for partnerships between civil government officials and private sector leaders to implement commercial solutions that provide uninterrupted access to PNT sources that strengthen the resilience of critical infrastructure.

Executive Order 13905[1], signed in 2020, states that it is essential to achieve national infrastructure resilience by backing up GPS with complementary PNT sources and promulgating best practices in cybersecurity through the responsible use of PNT. We agree that true resilience requires the widest possible diversity, and that is why one of our main objectives is to make certain that government requirements for PNT are sufficiently broad and include a range of technological solutions.

With the scope, complexity, and severity of disruptions and vulnerabilities evolving continuously, the combination of wide-ranging PNT solutions and emerging technologies offers superior protection to current and future threats by providing a backup to GPS and offering non-GPS forms of complementary PNT that improve national resilience.

Protecting critical infrastructure such as 5G networks depends on having multiple technologies to work alongside GPS or function in situations where GPS is degraded or denied, and to do so with the requisite properties of performance quality and operational resilience. The PNT landscape is expansive enough to allow

[1] Executive Order 13905 – *Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services* (February 2020) https://www.federalregister.gov/documents/2020/02/18/2020-03337/strengthening-national-resilience-through-responsible-use-of-positioning-navigation-and-timing

multiple and diverse complementary systems or approaches as alternatives to GPS with varied attributes to deliver against a complex and ever-expanding set of customer requirements.

Members of the alliance hold that a competitive marketplace is essential to provide full resilience, drive continuing innovation, and deliver cost-effective solutions. OPIA strongly recommends that the programs within the scope of the Public Wireless Supply Chain Innovation Fund acknowledge that the most robust GPS backup capabilities and complementary forms of PNT required by 5G networks are only possible through an open approach that encourages technology diversity throughout the industry.

PNT FOR 5G NETWORKS

The technical requirements for PNT in 5G networks have been documented in substantial detail by numerous engineering studies and industry white papers, so it is not necessary to repeat them here. However, the U.S. Government's own views and positions about PNT for 5G support why funding for PNT technologies should be addressed by the Public Wireless Supply Chain Innovation Fund.

OPIA strongly endorses the findings, recommendations, and guidelines of the following seminal PNT studies and urges them to be considered as part of the implementation of the Public Wireless Supply Chain Innovation Fund:

- The National R&D Plan for PNT Resilience[2] was most recently updated in 2021 and names Communications as a critical infrastructure sector that is not only highly dependent on PNT, but one that will cause other sectors to fail if it fails. Similarly, the most recent Federal Radionavigation Plan[3] referred to the Communications sector as a "lifeline function" that is "essential to the operation of most critical infrastructure sectors." These factors underscore how vitally important it is for 5G networks to have access to the broadest array of PNT technologies that meet the need when, where, and how such solutions are required.

- In its 2021 report[4] on complementary forms of PNT and technologies that back up GPS, the U.S. Department of Transportation cited takeaways from a wireless industry roundtable. Most notably the report explains that "modern communications networks require precise time and frequency standards to operate efficiently, with GPS being the most commonly deployed source of precise frequency control and absolute time distribution." Other determinations were that "wireless network providers are aware of GPS vulnerabilities," and "existing and emerging technologies can meet commercial timing requirements."

[2] The White House – *National R&D Plan for Positioning, Navigation, and Timing Resilience* (August 2021) https://www.whitehouse.gov/wp-content/uploads/2021/08/Position_Navigation_Timing_RD_Plan-August-2021.pdf

[3] U.S. Department of Defense, U.S. Department of Transportation, and U.S. Department of Homeland Security – 2021 Federal Radionavigation Plan (July 2022) https://rosap.ntl.bts.gov/view/dot/63024

[4] U.S. Department of Transportation – *Complementary Positioning, Navigation, and Timing (PNT) and GPS Backup Technologies Demonstration Report* (January 2021) https://www.transportation.gov/sites/dot.gov/files/2021-01/FY%2718%20NDAA%20Section%201606%20DOT%20Report%20to%20Congress_Combinedv2_January%202021.pdf

- A 2020 report[5] from the U.S. Department of Homeland Security stated that timing requirements with a minimal acceptable precision of anywhere between 65 and 240 nanoseconds supports all critical infrastructure requirements and is expected to meet future requirements, including 5G. DHS also said that "there are smart, market-oriented solutions that will contribute to enhanced resilience that the U.S. Government should continue to promote, enable, and stimulate."

- The 2020 National Space Policy[6] did not specifically call out 5G but stated that the U.S. Government shall "identify and promote, as appropriate, multiple and diverse complementary PNT systems or approaches for critical infrastructure and mission-essential functions."

The callouts highlighted above are just a few of the relevant PNT takeaways for 5G networks that can be found in these documents. **OPIA recommends that those U.S. Government personnel tasked with implementing the Public Wireless Supply Chain Innovation Fund should familiarize themselves with the full extent of the U.S. Government's PNT policies and publications to have a comprehensive understanding of PNT resilience principles that impact the Communications sector.**

Furthermore, with the Public Wireless Supply Chain Innovation Fund seeking to increase competition in the telecom market and promote the adoption of open, interoperable, and standards-based networks, we can expect many new technologies to emerge for 5G and its successors. This expanding variety of offerings will increase the need for different types of PNT, each with its own performance specifications and operational characteristics.

As the DOT said in its report referenced above, "suitable and mature technologies are available in the private sector and offer owners and operators of critical infrastructure a diverse array of complementary PNT services to meet their GPS backup needs. Because such needs are application-specific, GPS resilience across all critical infrastructure sectors will require a plurality of diverse PNT technologies to meet multiple use cases."

Given that robust PNT is a key enabler for the Communications sector, **OPIA recommends that NTIA should ensure that PNT from a range of different sources and provided by diverse technologies is accounted for in the deployment plans for next-gen networks, both 5G and beyond.** The types of PNT sources that can augment and complement GPS — even by working in conditions where GPS cannot — will be instrumental when deploying and operating wireless networks that are fast, versatile, and reliable.

TRIALS, PILOTS, USE CASES, AND MARKET DEVELOPMENT (Question Nos. 13 thru 16)

PNT technology is essential to U.S. communications networks, but too often it is viewed as an "invisible utility," with GPS sometimes taken for granted or PNT in general not being prioritized. Private sector operators of 5G networks have frequently deferred the adoption of complementary PNT technologies pending

[5] U.S. Department of Homeland Security – *Positioning, Navigation, and Timing (PNT) Backup and Complementary Capabilities to the Global Positioning System (GPS)* (April 2020) https://www.cisa.gov/sites/default/files/publications/report-on-pnt-backup-complementary-capabilities-to-gps_508_0.pdf

[6] The White House – *National Space Policy* (December 2020) https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/12/National-Space-Policy.pdf

a demonstrated commitment by the U.S. Government. Government leadership on the use of these commercially available PNT solutions will help spur private sector adoption of 5G as well as other national critical infrastructure.

OPIA recommends that the Public Wireless Supply Chain Innovation Fund should support industry activities and engagements that make 5G network operators aware of the GPS vulnerabilities and highlight the importance of an overall cybersecurity posture for PNT, help them evaluate solutions that enable resilient PNT, and educate them on solutions that are commercially available today.

As stated in the 2021 Federal Radionavigation Plan, "cost as well as user adoption is always a major consideration for owners and operators of critical infrastructure when contemplating non-GPS PNT investments." Members of the Open PNT Industry Alliance agree that getting critical infrastructure sectors to bring alternate forms of PNT online is a challenge because GPS is free. Yet having GPS at zero cost is not a great value in cases where the GPS signal is disrupted, manipulated, unavailable, or denied.

OPIA recommends that the Public Wireless Supply Chain Innovation Fund should be used to increase 5G resiliency by demonstrating the use of diverse, commercially available PNT technologies. Specifically, pilot programs should apply funding to progressively more wide-ranging small-, medium-, and large-scale deployments of backup and complementary PNT technologies. This would kick-start the responsible use of PNT within 5G operators. We believe that these projects would be easily scalable within available funding.

SECURITY (Question Nos. 17 thru 20)

One of the key aspects of Executive Order 13905 is its focus on the responsible use of PNT. Responsible use of PNT is defined as "the deliberate, risk-informed use of PNT services, including their acquisition, integration, and deployment, such that disruption or manipulation of PNT services minimally affects national security, the economy, public health, and the critical functions of the Federal Government."

Practicing the responsible use of PNT means not only having backups or complements to GPS in place and ready to go but also ensuring that PNT is part of any organization's cybersecurity posture. The U.S. Government has provided resources, tools, and guidance that can help wireless network operators establish and maintain high-performance platforms and systems that are also exceptionally resilient in the face of security threats.

OPIA encourages NTIA to incorporate security-oriented PNT principles from several authoritative sources into programs initiated through the Public Wireless Supply Chain Innovation Fund:

- The National Institute of Standards and Technology (NIST) introduced the Foundational PNT Profile[7] in 2021. Mandated by EO 13905 and built on the NIST Cybersecurity Framework, the Foundational PNT Profile brings the concept of responsible use of PNT to life. It gives security professionals within an

[7] National Institute of Standards and Technology – *Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services* (February 2021) https://csrc.nist.gov/publications/detail/nistir/8323/final

organization the tools and guidance to identify systems dependent on PNT, identify appropriate PNT sources, detect disturbances and manipulation of PNT services, and manage the risk to these systems.

- The U.S. Department of Homeland Security published the Resilient PNT Conformance Framework[8] that facilitates the development and adoption of expected behaviors in resilient PNT equipment through a common framework that enables improved risk management, determination of appropriate mitigations, and decision making by end-users.

- DHS also developed the PNT Reference Architecture[9] that incorporates the latest cybersecurity principles (e.g., zero trust) and combines them with PNT resilience concepts. It maps the Resilient PNT Conformance Framework levels to examples for how to implement.

OPIA recommends that the Public Wireless Supply Chain Innovation Fund support those programs that ensure not only that PNT systems enabling 5G are protected by cybersecurity measures that conform to the responsible use of PNT but also that PNT capabilities are themselves included as part of the broader cybersecurity construct for wireless operators.

SUMMARY

We have expressed our support for the Public Wireless Supply Chain Innovation Fund by explaining why diverse sources of PNT are important to 5G network operators, how program administrators can align with PNT policies from throughout the Federal Government, how funding can increase compliance with the responsible use of PNT, and what government guidelines and resources exist to help 5G providers improve their cybersecurity posture.

The Open PNT Industry Alliance looks forward to working with the U.S. Government on these matters, and we stand by ready to engage.

Very truly yours,

Kirk M. Vespestad
Facilitator
Open PNT Industry Alliance
kirk@openpnt.org
571-464-8934

[8] U.S. Department of Homeland Security – *Resilient Conformance Framework* (May 2022) https://www.dhs.gov/publication/st-resilient-pnt-conformance-framework

[9] U.S. Department of Homeland Security – *Resilient PNT Reference Architecture* (June 2022) https://www.dhs.gov/science-and-technology/publication/resilient-pnt-reference-architecture

Open PNT Industry Alliance Members

Aloft Sensing	www.aloftsensing.com
Echo Ridge LLC	www.echoridgenet.com
Focus Telecom	www.pnt-security.com
Geospatial Alpha	www.geospatialalpha.com
infiniDome Ltd.	www.infinidome.com
Iridium Communications Inc.	www.iridium.com
istlink	www.istlink.com.tr
Jackson Labs Technologies, Inc.	www.jackson-labs.com
NAVSYS Corporation	www.navsys.com
NextNav LLC	www.nextnav.com
OPNT B.V.	www.opnt.nl
Orolia	www.orolia.com
Oscilloquartz	www.oscilloquartz.com
OshoCorp Global Pvt. Ltd.	www.oshocorp.com
ProTrack	www.protrack.co.il
Qulsar, Inc.	www.qulsar.com
Satelles, Inc.	www.satelles.com
Seven Solutions S.L.	www.sevensols.com
Tallysman	www.tallysman.com
TrustPoint	www.trustpointgps.com
Xona Space Systems, Inc.	www.xonaspace.com

www.openpnt.org