OPEN PNT INDUSTRY ALLIANCE

POLICY VIEWS
MARCH 2025

A serious problem facing the United States and nations around the world is that the Global Positioning System (GPS) and other Global Navigation Satellite Systems (GNSS) are susceptible to inadvertent disruptions and deliberate attacks. Such incidents have the potential to impair or incapacitate communications networks, transportation systems, energy production and distribution platforms, financial services operations, and other types of critical infrastructure.

With the scope, complexity, and severity of disruptions and attacks evolving continuously, the combination of wide-ranging positioning, navigation, and timing (PNT) solutions and emerging technologies offers superior protection to current threats by providing backups to GPS/GNSS and improving national resilience. This is why companies from throughout the PNT market came together to form the Open PNT Industry Alliance (OPIA).

The Open PNT Industry Alliance is a coalition of manufacturers and service providers that provide what critical infrastructure needs for resilience: alternative forms of PNT that complement GPS/GNSS as well as augmentation services, security solutions, and hardware/software for PNT-dependent applications.

OPIA's mission is to promote open market concepts that preserve industry's long-term ability to harness its collective ingenuity to protect GPS/GNSS with multiple solutions that are technologically advanced, commercially viable, and based on a sustainable long-term funding framework.

The principal aim of the coalition is to ensure that critical infrastructure owners and operators have the freedom to adopt commercially available PNT solutions that best meet their operational needs. Additionally, OPIA works to ensure that government requirements for GPS/GNSS backup are sufficiently broad to include a range of technological solutions and that there are government commitments to policies and funding for the sustainability of diversified PNT solutions for critical infrastructure and national defense.

OPIA CORE PRINCIPLES AND BELIEFS

BUILDING RESILIENCE

The United States and other countries face a serious PNT resilience issue. True resilience requires the widest possible diversification, meaning that a singular sole-source technology will not only fail to meet the need in terms of reliability and performance but also be unable to evolve the optimal attack prevention and threat response capabilities.

PROMOTING HETEROGENEITY

The technological landscape is diverse enough to allow multiple alternatives to GPS/GNSS. Furthermore, each critical infrastructure sector has its own PNT performance specifications and operational characteristics — and today's PNT providers can deliver against a complex and ever-expanding set of customer requirements.

FOSTERING COOPERATION

National governments can set policy, define regulations, and enact legislation, but they may lack the technical expertise to effectively achieve their policy goals. The collective intellect of industry should be harnessed in a collaboration between the public sector and private sector to develop solutions at scale.

AVOIDING MONOPOLIES

As governments consider frameworks for regulation and funding, they can best pursue national interests through a multi-technology approach to PNT resilience and establishing a robust and self-sustaining funding framework that allows for the development and adoption of multiple sources of PNT that meet the needs of various sectors and industries.

PREPARING FOR THE FUTURE

The inventiveness of the private sector, spurred by competition and public and private investment, has driven the emergence of multiple cost-effective GPS/GNSS augmentations and alternatives that evolve according to technological innovations and market dynamics. Similarly, unrestrained innovation will address new and evolving use cases not supported by GPS/GNSS.

DEVELOPING SENSIBLE MODELS

The Federal Government should build upon the U.S. Department of Transportation's Complementary PNT Action Plan by implementing the process for procuring CPNT technologies. This important step will not only spur adoption by critical infrastructure owners and operators to protect PNT-dependent applications but also preserve and expand the ability of companies in the private sector to innovate across the gamut of current and future use cases.

We need many backups for GPS, not just one.

GPS and those who use it must have a contingency plan in case it becomes degraded, disrupted, deceived, or denied. Critical infrastructure owners and operators and other enterprise-class organizations with PNT-dependent applications need access to multiple and diverse sources of positioning, navigation, and timing information.

Each critical infrastructure sector has different needs. A mosaic of complementary PNT technologies to back up GPS is more in the public interest, so we agree with DHS that it "could not identify generic specifications for a national backup" because "[t]he position and navigation functions in critical infrastructure are so diverse that no single PNT system, including GPS, can fulfill all user requirements and applications."

DOT agreed by stating, "The critical infrastructure positioning and navigation requirements are so varied that function, application, and end-user specific positioning and navigation solutions are needed. This necessitates a diverse universe of positioning and navigation technologies."

Alternatives exist today, and there are more on the horizon.

DHS notes that "critical infrastructure systems that would cease to operate without [the primary PNT domain of] GPS do so because of design choices, cost factors, increasing efficiency, or other considerations—not because of a lack of available additional means to navigate, determine location, or synchronize." As DHS goes on to say, "there are smart, market-oriented solutions that will contribute to enhanced resilience that the U.S. Government should continue to promote, enable, and stimulate."

DOT again expressed agreement with DHS, stating that "[T]here are suitable, mature, and commercially available technologies to backup or complement the timing services provided by GPS [, but that] none of the systems can universally backup the positioning and navigations capabilities provided by GPS and its augmentations."

Competition must thrive to drive innovation.

The Federal Government should neither provide nor select a single PNT solution; rather, it should encourage diverse solutions and invest in multiple technologies. Regarding any kind of government preference for a particular PNT system, DHS states that "the government would have to consider the repercussions of such a system in the marketplace" because "[a] free government system would negatively impact commercially available PNT systems by directly competing with them."

OPIA's view is that a truly resilient and globally available GPS backup capability is only possible with an open, technology-neutral approach that encourages a diversity of solutions. We agree with DHS that "[t]he Federal Government should encourage adoption of multiple PNT sources [by] critical infrastructure owners and operators [and] focus on facilitating the availability and adoption of PNT sources in the open market." What's more, partnerships and collaborations between players in the PNT market will promote further innovation.

The Federal Government can help by showing the way.

OPIA members have seen that commercial implementation will not happen absent directives and requirements from the U.S. Government. "[W]ithout regulatory requirements or positive benefit-cost equations, adoption of non-GNSS services is unlikely," stated DHS, adding that "business decisions, the lack of a Federal mandate, and potentially an underappreciation of the risk associated with GPS dependence are factors in the lack of resilience to GPS disruption."

DHS is taking action, such as through its development of the Resilient PNT Reference Architecture, supporting efforts by the Federal Government to protect itself by providing guidance to agencies for how to procure technologies that bring about PNT resilience, and promoting PNT resilience best practices that can be

implemented in all critical infrastructure sectors. DOT's PNT Strategic Plan defines the big picture view for resilient PNT throughout the nation, and its Complementary PNT Action Plan provides the blueprint for how to achieve resilience through industry adoption of various forms of PNT. And NIST, through the Foundational PNT Profile, has applied its robust cybersecurity framework to help practitioners achieve resilience.

We need even more action from the Federal Government: clear direction, the freedom to choose the technology that best meets each individual requirement, and the funding to stimulate the adoption of resilient PNT technologies throughout our critical infrastructure.

The Federal Government can also help by eliminating uncertainty.

Many critical infrastructure owners and operators are hesitant to invest in the diverse solutions that can meet the needs today for fear that the Federal Government will at some point mandate the use of a single national backup. Essential enterprises are failing to act with speed and commitment because they are of the belief that "something else" is coming.

In addition to providing the kind of support that will allow multiple forms of PNT to flourish, the Federal Government should more clearly and boldly articulate that its strategy is to promote a diversified array of technologies rather than mandate only one. The market needs to be confident that it is acceptable to not only adopt the solutions that exist today but also consider the ones that are poised to move out of the lab and into the field. This confidence will compel them to embrace the responsible use of PNT with conviction.

References

The White House, Executive Order 13905 – Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services (February 12, 2020), https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-strengthening-national-resilience-responsible-use-positioning-navigation-timing-services/

U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, Report on Positioning, Navigation, and Timing (PNT) Backup and Complementary Capabilities to the Global Positioning System (GPS) (submitted to U.S. congressional committee leaders on April 8, 2020; released to the public on May 6, 2020), https://www.cisa.gov/sites/default/files/publications/report-on-pnt-backup-complementary-capabilities-to-gps_508_0.pdf

U.S. Department of Transportation, Complementary 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

U.S. Department of Transportation, Complementary PNT Action Plan (September 2023; updated March 2024), https://www.transportation.gov/sites/dot.gov/files/2024-03/DOT%20Complementary%20PNT%20Action%20Plan_Final_Updated_March%202024.pdf

U.S. Department of Transportation, PNT Strategic Plan (January 17, 2025), https://www.transportation.gov/pnt/dot-positioning-navigation-timing-pnt-strategic-plan