Before the Department of Commerce
National Institute of Standards and Technology
Washington, D.C.

In the Matter of	)	
	)	
Profile of Responsible Use of	)	Docket Number 200429–0124
Positioning, Navigation, and Timing	)	
Services	)	

COMMENTS OF CTIA

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

Melanie K. Tiano
Director, Cybersecurity and Privacy

CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200
www.ctia.org

July 13, 2020

TABLE OF CONTENTS

I. INTRODUCTION & SUMMARY 3

II. NIST SHOULD USE WIRELESS INDUSTRY EXPERTISE IN DEVELOPING THE PNT PROFILE. 4

A. The Communications Sector Relies on PNT Services. 4

B. The Wireless Industry Manages PNT Security and Reliability. 6

C. Innovation in GPS and Alternatives Continues to Evolve. 9

III. NIST CAN BUILD ON PRIOR EFFORTS TO SECURE PNT AND WORK CLOSELY WITH THE COMMUNICATIONS SECTOR. 10

A. NIST Should Promote Public-Private Sector Collaboration With the Communications Sector on PNT Security. 10

B. DHS is the Sector Specific Agency for the Communications Sector, so its Collaboration with the Private Sector will be Critical. 12

C. NIST Should Heed the Many Other Efforts on PNT. 14

IV. NIST SHOULD APPROACH THE PNT PROFILE AS IT DID THE CYBERSECURITY FRAMEWORK. 15

A. A Voluntary and Flexible Profile Should Account for Cost and Feasibility. 16

B. NIST Should Recognize that Any Procurement Requirements Need to be Carefully Considered and Should Not be One-Size-Fits-All. 16

C. Vulnerability Assessments and Testing Should be Handled with Caution and Confidentiality. 17

V. CONCLUSION 18

Before the Department of Commerce
National Institute of Standards and Technology
Washington, D.C.

In the Matter of)
)
Profile of Responsible Use of) Docket Number 200429–0124
Positioning, Navigation, and Timing)
Services)

COMMENTS OF CTIA

I. INTRODUCTION & SUMMARY

CTIA[1] welcomes the opportunity to engage with the National Institute of Standards and Technology ("NIST") on its request for information ("RFI") on the *Profile of Responsible Use of Positioning, Navigation, and Timing* ("PNT") *Services*.[2] The February 2020 Executive Order ("EO") directed the Secretary of Commerce to develop a PNT profile that "will enable the public and private sectors to identify systems, networks, and assets dependent on PNT services; identify appropriate PNT services; detect the disruption and manipulation of PNT services; and manage the associated risks to the systems, networks, and assets dependent on PNT services."[3]

As users and innovators of PNT services and the Global Positioning System ("GPS"), CTIA and its members are encouraged that the profile "will be developed using an open and

[1] CTIA – The Wireless Association® ("CTIA") (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st century connected life. The association's members include wireless carriers, device manufacturers, suppliers as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

[2] NIST, Request for Information, 85 Fed. Reg. 31743 (May 27, 2020) ("*RFI*"), https://www.govinfo.gov/content/pkg/FR-2020-05-27/pdf/2020-11282.pdf.

[3] The White House, Executive Order 13905, *Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services* (Feb. 12, 2020), https://www.whitehouse.gov/presidential-actions/executive-order-strengthening-national-resilience-responsible-use-positioning-navigation-timing-services/. ("EO").

collaborative process involving public and private sector stakeholders."[4] Research and innovation in alternatives and mitigations are ongoing, so flexibility is paramount.

CTIA offers input on "standards, practices, and technologies used to manage cybersecurity risks, to systems, networks, and assets dependent on PNT services."[5] The wireless industry prioritizes resilient networks and devices. In these comments, CTIA:

- Outlines security resiliency built in to mitigate risks in PNT services;
- Shares recent network and device security enhancements;
- Outlines ongoing efforts that NIST should consider in its PNT Profile; and
- Urges NIST to develop the Profile as it did the Cybersecurity Framework, building consensus around flexible and voluntary approaches.

II. NIST SHOULD USE WIRELESS INDUSTRY EXPERTISE IN DEVELOPING THE PNT PROFILE.

A. The Communications Sector Relies on PNT Services.

As stated in the EO, "[s]ince the United States made the Global Positioning System available worldwide" space-based PNT services have become a "largely invisible utility for technology and infrastructure, including the electrical power grid, communications infrastructure and mobile devices" as well as transportation, agriculture, weather forecasting, and emergency response.[6] The U.S. government recognizes that "[p]recise time is crucial to a variety of economic activities around the world. Communication systems, electrical power grids, and financial networks all rely on precision timing for synchronization and operational efficiency."[7]

Most smartphones and connected devices have integrated GPS to support mobile applications[8] and emergency calls. And "wireless telephone and data networks use GPS time to

[4] RFI at 31744.
[5] *Id.* at 31743.
[6] EO
[7] GPS.gov, *Timing*, available at: https://www.gps.gov/applications/timing/.
[8] *See, e.g.*, GPS.gov, *Recreation*, available at: https://www.gps.gov/applications/recreation/.

keep all of their base stations in perfect synchronization. This allows mobile handsets to share limited radio spectrum more efficiently."[9] Networks also provide assisted or augmented-GPS for wireless terminals.

> GPS receivers are essential to the telecom industry: [t]he U.S. telecommunications industry has deployed a large number of GPS receivers and is constantly adding new receivers each year as the network grows, especially in wireless. These GPS receivers, which have a lifetime of more than 15 years, are used for precision timing from fixed locations. Based on industry estimates, fewer than 5% of these units are used to support optical networks and more than 95% are used to support the fixed infrastructure for wireless (*i.e.*, wireless base stations – Code Division Multiple Access ("CDMA"), Long-Term Evolution ("LTE"), and Enhanced 9-1-1 "E911") augmentation systems). The telecommunications industry is dependent on these receivers for precision time accuracy.[10]

Communications networks are important for a host of GPS and PNT services that relate to public safety and disaster relief.[11] In an emergency, the ability to locate wireless 911 callers quickly and accurately is of critical importance to first responders and those they help. Using a smartphone's GPS coordinates, E911 helps to route emergency providers to the caller. For more than a decade, the Federal Communications Commission ("FCC") has worked with industry, commercial mobile radio service ("CMRS") providers, and the public safety community to ensure the accuracy of E911. The FCC's wireless E911 rules address the effectiveness and reliability of wireless 911 services by providing 911 dispatchers with information on wireless 911 calls, including location data.[12]

Additionally, accurate time is important in cybersecurity generally—to authenticate and verify networks users, devices, and systems. The Communications Sector plays an important role in resiliency and security in systems reliant on PNT services, and, as the government has

[9] GPS.gov, *Timing*, available at: https://www.gps.gov/applications/timing/.

[10] ATIS, *GPS Vulnerability* (2017), https://access.atis.org/apps/group_public/download.php/36304/ATIS-0900005.pdf..

[11] GPS.gov, *Safety*, available at: https://www.gps.gov/applications/safety/.

[12] *See* FCC, *911 and E911 Services*, available at: https://www.fcc.gov/general/9-1-1-and-e9-1-1-services.

recognized, the Communications Sector, in addition to being a recognized critical infrastructure sector on its own, performs an enabling function across other sectors.[13] Thus for PNT service, any evaluation should include the impacts of disruption on all critical infrastructure sectors.

B. The Wireless Industry Manages PNT Security and Reliability.

NIST seeks information about the use of PNT and the cybersecurity risk management approaches used to protect services, in order "[t]o bolster the resilience of [GPS] and the wide scope of technologies and services that rely on precision timing."[14] As outlined above, the wireless industry uses PNT services in networks, products, and services. Given the size and variety of wireless networks and providers, it is important that the industry has commercially available solutions that are cost effective, and scalable across all switches and cell site locations.

The wireless industry implements a variety of technologies to secure networks and to mitigate the risk of GPS outages. Through network rerouting, device-based navigation and timing capabilities, and cloud-based or software-based applications, wireless providers can respond to GPS outages and continue voice and data transmissions. NIST should consider these existing capabilities in developing the PNT Profile. GPS interruptions are not uncommon, and the wireless industry manages them without significant disruption.

There are myriad mechanisms in place to address PNT security and reliability. The Department of Homeland Security's ("DHS") Cybersecurity and Infrastructure Security Agency ("CISA") distributes notices of GPS testing and interruptions on a regular basis. GPS.gov reports on GPS service interruptions, and the Coast Guard Navigation Center addresses reports of

[13] *See* Presidential Policy Directive 21.

[14] NIST, *NIST Seeks Public Input on Use of Positioning, Navigation and Timing Services* (May 27, 2020), available at: https://www.nist.gov/news-events/news/2020/05/nist-seeks-public-input-use-positioning-navigation-and-timing-services.

problems.[15] DHS "recommends that responsibility for mitigating temporary-GPS outages be the responsibility of the individual user and not the responsibility of the Federal Government. Research [shows] that users can mitigate short-term GPS disruptions (*e.g.*, inability to read a GPS signal) with various strategies, ranging from using local backup capabilities to delaying operations until GPS is restored."[16] As discussed in another DHS white paper, *Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure*, securing PNT services is done using "[s]trategies that can result in more resilient new and/or improved products based on existing technology and knowledge."[17]

Among other things, DHS found that "receivers and equipment today and existing techniques … can be inserted into new products. These installation and operation strategies and development opportunities … can significantly enhance the ability of [Global Navigation Satellite System ("GNSS")] receivers and associated equipment to defend against a range of interference, jamming, and spoofing attacks."[18] In addition to the recommendations outlined by DHS, there are accepted security practices and mitigations that can reduce threats to systems reliant on PNT services.

- ***Testing systems for vulnerabilities***. Testing protocols can simulate a spoofing, jamming or denial of service attack to evaluate how networks or systems respond. Establishing if and where particular vulnerabilities may be in unique systems can help build more resilient PNT, and aid in the design of enhanced solutions.
- ***Ongoing monitoring of systems***. Threat monitoring systems have been deployed by the private sector to monitor signals, detect interference, and notify engineers and security personnel of possible issues. PNT services and GNSS monitoring systems can help

[15] *See, e.g.* GPS.gov, *GPS Service Outages & Status Reports*, available at: https://www.gps.gov/support/user/.
[16] DHS, *Report on Positioning, Navigation, and Timing (PNT) Backup and Complementary Capabilities to the Global Positioning System (GPS)* (Apr. 8, 2020) available at: https://www.cisa.gov/sites/default/files/publications/report-on-pnt-backup-complementary-capabilities-to-gps_508.pdf.
[17] DHS, *Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure*, available at: https://www.navcen.uscg.gov/pdf/gps/Best%20Practices%20for%20Improving%20the%20Operation%20and%20Development%20of%20GPS%20Equipment.pdf
[18] *Id.*

identify the type of threat and mitigate it, depending on the nature of the threat, by filtering the signal to neutralize interference.[19]

- ***Denying interfering signals access to the receiver***. Some security systems can neutralize interference. PNT-reliant services may also possess "smart antenna technology which focuses antenna beams to track the good signals from the satellites and reject the bad signals from interferers. Less sophisticated solutions such as blocking antennas can be employed to reject terrestrial-based interference, which is where most GNSS interference sources exist, and they provide a good first-level protection."[20]
- ***Developing backups and alternatives***. "Continuous PNT access can also be achieved by using an alternative signal that operates separately from GPS/GNSS and is less vulnerable to the signal attacks that plague GNSS signals."[21] Many wireless networks have an atomic clock that keeps accurate time for network synchronization if there is a GPS outage. And if a GPS outage is local, GPS timing can be relayed over fiber from locations not affected by the outage. Some networks are making use of the other GPS bands, such as the L5 band to provide additional resiliency, beyond the L1 band. "Alternative signals are now available, and these new signal options, such as STL (Satellite Time and Location), could play an important role in providing better privacy and security functionality. This signal diversity will help protect against threats and interference by adding resilience to the device's ability to receive reliable PNT data."[22]

GPS.gov, the official federal source for information on GPS and related topics, has released best practices and research. In April 2020, the government released the 5th Edition of the GPS Standard Position Service ("SPS") Performance Standard, which "defines the levels of performance the U.S. Government makes available to users of the [GPS SPS]."[23] In its guidance, "U.S. government strongly encourages all GPS users to maintain backup/alternative positioning, navigation, and timing capabilities."[24] Wireless carriers maintain backups and alternatives to support more resilient communications services. During loss or interruption of GPS timing, carriers can rely on highly precise internal networks to maintain services.

The wireless industry is on the cutting edge of security, and fifth generation ("5G")

[19] *See, e.g.*, Sarang Thombre, *et al.*, Cambridge University Press, *GNSS Threat Monitoring and Reporting: Past, Present, and a Proposed Future* (Dec. 2017).

[20] Rohit Bragg, GPS World, *How resilient PNT protects global networks from attack or failure* (June 2019) available at: https://www.gpsworld.com/how-resilient-pnt-protects-global-networks-from-attack-or-failure.

[21]*Id.*

[22] *Id.*

[23] 5th Edition of the GPS Standard Position Service Performance Standard (Apr. 2020) available at: https://www.gps.gov/technical/ps/2020-SPS-performance-standard.pdf.

[24] GPS.gov, *FAQs*, available at: https://www.gps.gov/support/faq/#jamming.

wireless technology will bring substantial enhancements to the overall ecosystem, including PNT systems and services. Wireless and network innovations will enable more nimble and flexible responses that can mitigate risks related to PNT services, from device security enhancements to network slicing and software defined networks that can enhance redundancy and recovery. Any PNT Profile should consider these and other security advancements in the wireless sector.

C. Innovation in GPS and Alternatives Continues to Evolve.

Standards bodies have produced best practices for PNT.[25] Existing standards apply to different uses cases and scenarios but are in use and could aid in the development of the PNT Profiles. No standards or best practices should be set in stone and PNT Profiles should allow for creative alternatives and evolving developments. WiFi positioning systems, which are being used more widely, could be used as temporary or supplemental alternatives. These systems can provide geolocation indoors, where GPS signals may not be able to reach.

5G technologies and the Internet of Things ("IoT") will need to integrate with GPS, which will be necessary for evolving applications and future uses. 5G's increased capacity, higher speeds, and lower latency will support billions of devices that will need to know where they are and what time it is. Applications ranging from smart cities, automated and driverless cars, smart energy grids, precision agriculture sensors, telemedicine, and more will require 5G speeds and throughput and rely on GPS or possible alternatives.

Private and academic research into PNT alternatives and resiliency is ongoing at places like Stanford Engineering's GPS lab.[26] The federal government, including the U.S. Army, is

[25] *See, e.g.* ITU-T Recommendation G.8271, Time and phase synchronization aspects of packet networks. ITU-T Recommendation G.8272, Timing characteristics of primary reference time clocks. ITU-T Recommendation G.8272.1, Timing characteristics of enhanced primary reference time clocks. ITU-T Recommendation J.211, Timing interface for cable modem termination systems. IEEE Std 1588 – 2008, IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems.

[26] *See* Stanford Engineering GPS Lab, *Alternative PNT*, available at: https://gps.stanford.edu/research/current-research/alternative-pnt.

looking at alternative options to PNT.[27] NIST should consider these developments.

III. NIST CAN BUILD ON PRIOR EFFORTS TO SECURE PNT AND WORK CLOSELY WITH THE COMMUNICATIONS SECTOR.

A. NIST Should Promote Public-Private Sector Collaboration With the Communications Sector on PNT Security.

NIST should draw on public and private sector partnerships aimed at securing PNT services to support security in the PNT ecosystem and avoid duplication of efforts. Multiple prior efforts can be built upon. The FCC's Communications Security, Reliability and Interoperability Council ("CSRIC") V, led by wireless stakeholders, developed an analysis of backup options in the case of GPS outages. CSRIC V, Working Group 4 (Network Timing Single Source Risk Reduction) explored complementary and backup options, identifying technical, security, and cost issues, which NIST should consider along with more recent developments.[28]

The CSRIC noted that wireless carriers deploy a "wide range of timing and frequency standards"[29] and deploy high-quality timing-grade radio-navigation satellite services to reduce the cost and distribution burdens of maintaining multiple low-stratum references in their networks. NIST should consider the ongoing subscription and equipment costs and potential effectiveness challenges of the eLORAN option, as described by CSRIC V.[30] In 2018, the President signed the Frank LoBiondo Coast Guard Authorization Act of 2018,[31] which includes as Section 514 the National Timing Resilience and Security Act of 2018, which amends Title 49 of the U.S. Code to include the following language:

[27] Dee Ann Davis, Inside GNSS, *Army Seeks More Alternative PNT Options*, available at: https://insidegnss.com/army-seeks-more-alternative-pnt-options/.

[28] See CSRIC V, WG4B Presentation (Dec. 21, 2016), available at: https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability.

[29] *Id.* at Sec. 2.1.

[30] *See id.* at Section 3.0 and Table 4-1 (citing costs and lack of effectiveness of eLORAN relative to GPS).

[31] *See* P.L. 115-282 (2018).

> § 312. Alternative timing system
>
> (a) In General.—Subject to the availability of appropriations, the Secretary of Transportation shall provide for the establishment, sustainment, and operation of a land-based, resilient, and reliable alternative timing system—
>
> (1) to reduce critical dependencies and provide a complement to and backup for the timing component of the Global Positioning System (referred to in this section as 'GPS'); and
>
> (2) to ensure the availability of uncorrupted and non-degraded timing signals for military and civilian users in the event that GPS timing signals are corrupted, degraded, unreliable, or otherwise unavailable.

The act goes on to provide specific direction about the establishment of requirements; implementation plan; LORAN facilities; and agreement authority.[32]

The Alliance for Telecommunications Industry Solutions ("ATIS") has provided guidance to the U.S. government in 2020 on PNT security and is actively working on these issues.[33] A technical working group in ATIS produced a report on *GPS Vulnerability*, offering "a North American telecom sector perspective on the impact of GPS vulnerabilities to telecom networks, synchronization in particular" and "recommendations for consideration by the larger timing community."[34] This 2017 report outlined proposals to mitigate GPS vulnerabilities on critical infrastructure receivers, using :

- Navigational Message Authentication on modernized GPS civil signals
- Atomic clock time holdover
- Sync over fiber
- eLoran
- WWVB
- Terrestrial beacons
- Communication satellite timing
- Differential time transfer[35]

[32] *See* GPS.gov, *LORAN-C Infrastructure & E-LORAN*, available at: https://www.gps.gov/policy/legislation/loran-c/.

[33]GPS.gov, *Presentation from ATIS Time & Money Conference* (2020) available at: https://www.gps.gov/multimedia/presentations/2020/ATIS/; *see also* ATIS, *Timing Security: Mitigating Threats in a Changing Landscape Webinar* (2018) available at: https://www.atis.org/01_news_events/webinar-pptslides/Timing-Security5222018.pdf.

[34] ATIS, *GPS Vulnerability* (2017) available at: https://access.atis.org/apps/group_public/download.php/36304/ATIS-0900005.pdf.

[35] *Id*. at 14.

ATIS also made specific recommendations for the U.S. Government, that federal agencies responsible for GPS should consider adding signal-side security features, such as Navigation Message Authentication ("NMA"), to the L2C, and L5 Modernized Civil Signals as a possible mitigation strategy against spoofing attacks on civil GPS signals. ATIS further recommended that NIST and USNO empower scientists and engineers to work with industry on GPS vulnerability and backup issues.[36] Two sections of the report may be particularly relevant:

- Section 7 describes GPS vulnerability mitigation and alternatives to GPS timing that are generally applicable to critical infrastructure sectors; and
- Section 8 provides recommendations to help define PNT profiles relevant to the telecommunications industry.

NIST should use the most up-to-date information in developing the PNT Profile and seek guidance on recent developments.

B. DHS is the Sector Specific Agency for the Communications Sector, so its Collaboration with the Private Sector will be Critical.

DHS plays an important role, working with the private sector and the Communications Sector. DHS has an MOU with the Department of Defense and other agencies to manage PNT issues.[37] The DHS PNT Interference, Detection and Mitigation Plan ("IDMP") Implementation Strategy directed the development of plans to coordinate federal capabilities to identify interference affecting GPS-provided PNT services.

CISA manages reporting of GPS interruptions and the Science and Technology Directorate ("S&T") also plays a role. S&T "recognizes the importance of accurate and precise [PNT] information to critical infrastructure and has a dedicated multi-year program to address

[36] *See id.*

[37] GPS.gov, *Interagency Memorandum of Agreement With Respect to Support to Users of The Navstar Global Positioning System (GPS),* available at: https://www.gps.gov/policy/docs/2017/user-support-MOA/

GPS vulnerabilities in critical infrastructure, with a multi-pronged approach of conducting vulnerability and impact assessments, developing mitigations, exploring complementary timing technologies, and engaging with industry through outreach events and meetings."[38] S&T maintains a program with the goal of increasing the resiliency of critical infrastructure to GPS vulnerabilities in the future.[39]

Collectively, these efforts result in a great deal of DHS work on PNT. In May 2020, DHS issued a report on *PNT Backup and Complementary Capabilities to the GPS*.[40] In 2019, DHS published its list of National Critical Functions ("NCFs"), which included providing PNT services as a key risk under the "Connect" function.[41] Even before establishing NCFs, DHS looked at risks to GPS. In 2018, the Director of DHS's PNT Program Office briefed the National PNT Advisory Board on the DHS's plans to address GPS technologies.[42]

DHS S&T dedicated a multi-year program to GPS vulnerabilities in critical infrastructure, with a multi-pronged approach to: conduct vulnerability and impact assessments; develop mitigations; explore complementary timing technologies; and engage with industry. [43] DHS S&T released best practices. *Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure* identified threats from

[38] *See* DHS Notice, *2020 GPS Equipment Testing for Critical Infrastructure* (Mar. 2020) available at: https://beta.sam.gov/opp/1942578638c542239fc04851f252f6f6/view.

[39] *See* DHS S&T, *Position, Navigation, and Timing (PNT) Program*, available at: https://www.dhs.gov/science-and-technology/pnt-program.

[40] *See* CISA, *Report on PNT Backup and Complementary Capabilities to the GPS* (May 5, 2020) available at: https://www.cisa.gov/publication/pnt-backup-report.

[41] CISA, *National Critical Functions Set* (Apr. 2019) available at: https://www.cisa.gov/sites/default/files/publications/national-critical-functions-set-508.pdf.

[42] *See* GPS.gov, December 2018 PNT Advisory Board Meeting (Dec. 2018) available at: https://www.gps.gov/governance/advisory/meetings/2018-12/platt.pdf

[43] *See* DHS S&T, *Snapshot: S&T is Working to Address GPS Vulnerabilities, Improving Critical Infrastructure Resilience*, available at: https://www.dhs.gov/science-and-technology/news/2018/11/30/snapshot-st-working-address-gps-vulnerabilities

interference, jamming, and spoofing, whether inadvertent, naturally occurring, or malicious.[44] Among its findings, DHS proposed "recommendations [that] focus on steps owners, operators, and third-party installers can take, external to the equipment, that can be employed immediately on current equipment. Implementation of these strategies should use best judgment based on application- and site-specific information."[45] DHS listed 22 recommendations for owners, operators, installers, and manufacturers, including:

- Installation and operation strategies that can be implemented for current equipment; and
- Multiple strategies that can result in more resilient new and/or improved products based on existing technology and knowledge.

In an earlier publication, DHS's US-CERT released *Best Practices for Improved Robustness of Time and Frequency Sources in Fixed Locations*.[46] DHS plans a 2020 event related to GPS Equipment Testing for Critical Infrastructure and DHS S&T hosts GPS Equipment Testing for Critical Infrastructure (GET-CI) to give researchers, industry partners, and stakeholders an opportunity to test and evaluate their equipment in a Live-Sky environment.[47] If anything, DHS's work with the private sector on PNT could be better coordinated, so that alerts and information are better disseminated to the private sector.

C. NIST Should Heed the Many Other Efforts on PNT.

Other NIST efforts and public-private partnerships can be leveraged. In March 2019 NIST and MITRE hosted a workshop to develop "a Conformance Framework applicable to the

[44] *See* DHS, *Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure*, available at: https://www.navcen.uscg.gov/pdf/gps/Best%20Practices%20for%20Improving%20the%20Operation%20and%20Development%20of%20GPS%20Equipment.pdf. .

[45] *Id.*

[46] *See* DHS, *Best Practices for Improved Robustness of Time and Frequency Sources in Fixed Locations* (2015) available at: https://us-cert.cisa.gov/sites/default/files/documents/Best%20Practices%20-%20Time%20and%20Frequency%20Sources%20in%20Fixed%20Locations_S508C.pdf.

[47] *See DHS, 2020 GPS Equipment Testing for Critical Infrastructure* (Mar. 25, 2020) available at: https://beta.sam.gov/opp/d3489175b4544508acdae10f91769b7b/view.

question of providing the US critical infrastructure access to accurate and assured time."[48] NIST also hosted a webinar on the EO, this RFI, and the development of the PNT Profile.[49]

The National Space-Based Positioning, Navigation, and Timing Advisory Board "provides independent advice to the U.S. government on GPS-related policy, planning, program management, and funding profiles in relation to the current state of national and international satellite navigation services"[50] and noted the EO's publication. The Civil GPS Service Interface Committee ("CGSIC") was established by Department of Transportation ("DOT") to exchange information about GPS with the civil user community, respond to the needs of civil GPS users, and integrate GPS into civil sector applications. CGSIC includes members from U.S. and international private, government, and industry groups.[51] DOT works with DHS and DoD "to increase awareness of vulnerabilities of GPS, to evaluate the impacts, and to research complementary sources of PNT to increase resiliency for safety-critical transportation applications. DOT coordinates research on technologies to address emerging PNT needs for applications across all modes of transportation, such as autonomous vehicles. Recently the Department of Commerce's Bureau of Industry and Security listed PNT as an area that it might subject to export controls.[52] PNT is getting attention across government. These efforts should be more coordinated and unified.

IV. NIST SHOULD APPROACH THE PNT PROFILE AS IT DID THE CYBERSECURITY FRAMEWORK.

[48] *See* NIST, *Access to Assured and Accurate Time II: Assuredness of Reference Architectures*, available at: https://www.nist.gov/news-events/events/2019/03/access-assured-and-accurate-time-ii-assuredness-reference-architectures

[49] *See* NIST, *Responsible Use of Positioning, Navigation, and Timing Services*, available at: https://www.nist.gov/itl/pnt.

[50] *See* GPS.gov, *National Space-Based Positioning, Navigation, and Timing Advisory Board* https://www.gps.gov/governance/advisory/.

[51] *See* GPS.gov, *CGSIC*, available at: https://www.gps.gov/cgsic/.

[52] *See* BIS, *ANPRM on Review of Controls for Certain Emerging Technologies* (Dec. 19, 2018) available at: https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies.

A. A Voluntary and Flexible Profile Should Account for Cost and Feasibility.

The goal of NIST's PNT Profile is to help organizations identify systems, networks, and assets that depend on PNT services, detect the disruption and manipulation of PNT services, and manage the associated risks. This profile is to "be developed using an open and collaborative process" with public and private sector stakeholders.[53] NIST should encourage stakeholder engagement by holding public forums and creating opportunities, in coordination with DHS, for stakeholders in more private settings to discuss risks openly. Risk-based frameworks should recognize that threats and mitigations will vary depending on the industry and users. As the PNT Profile takes shape, NIST should reiterate its voluntary and flexible nature for the private sector.

As with any risk management framework, cost and feasibility should be factors. Possible alternatives to GPS may not be feasible under certain circumstances. Any terrestrial GPS backup option will require a significant deployment of antennas on our nation's wireless infrastructure. This may require further engagement with tower company owners and operators so any demonstration can address tower space availability and operational issues.

B. NIST Should Recognize that Any Procurement Requirements Need to be Carefully Considered and Should Not be One-Size-Fits-All.

Section 4(d) of the EO directs the development of "contractual language for inclusion of the relevant information from the PNT profiles in the requirements for Federal contracts for products, systems, and services that integrate or utilize PNT services."[54] Part of the goal is to

[53] *See* NIST, *Responsible Use of Positioning, Navigation, and Timing Services,* available at: https://www.nist.gov/itl/pnt.

[54] *EO* ("Within 90 days of the PNT profiles being made available, the heads of SSAs and the heads of other executive departments and agencies (agencies), as appropriate, through the Secretary of Homeland Security, shall develop contractual language for inclusion of the relevant information from the PNT profiles in the requirements for Federal contracts for products, systems, and services that integrate or utilize PNT services, with the goal of encouraging the private sector to use additional PNT services and develop new robust and secure PNT services. The heads of SSAs and the heads of other agencies, as appropriate, shall update the requirements as necessary.")

encourage the private sector to "use additional PNT services and develop new robust and secure PNT services." Before new obligations are created, NIST, DHS and sector specific agencies ("SSAs") need to consider use cases and flexible solutions that recognize different risks and needs. They also need to be aware of ongoing private research to verify that meaningful and feasible solutions exist. DHS S&T identified mitigations for resilient PNT services, ranging from "implementing best practices to developing improved, more secure hardware. Examples include improving situational awareness by developing the capability to detect and automatically alert users of jamming or spoofing events, working with equipment manufacturers to ensure newer product lines are more robust to existing threats, and developing new antenna designs optimized to minimize jamming and spoofing effects on GPS receivers."[55]

DHS S&T has underscored the importance of ongoing stakeholder engagement at all stages. "A key element of [more resilient PNT services] is outreach to stake-holders to educate them on threats, vulnerabilities, impacts, and mitigations. Equipment manufacturers and critical infrastructure owners and operators are a crucial part of this effort."[56] As a result, procurement determinations should be flexible, to allow for a diversity of technologies and solutions.[57]

C. Vulnerability Assessments and Testing Should be Handled with Caution and Confidentiality.

The EO, section 4(c), envisions DHS and the heads of SSAs developing "a plan to test the vulnerabilities of critical infrastructure systems, networks, and assets in the event of disruption and manipulation of PNT services." It also directs that the results of those tests be

[55] DHS S&T, *Resilient PNT for Critical Infrastructure*, https://www.dhs.gov/sites/default/files/publications/resilient_pnt_for_critical_infrastructure_fact_sheet_508.pdf

[56] *Id.*

[57] *Id.* ("In addition to mitigation capabilities…complementary timing technologies [can] reduce reliance on a single system (i.e. GPS)…Alternative timing technologies will not only provide new sources of robust timing data, but they will also hamper jamming and spoofing attempts, as having complementary timing sources enables comparison and validation of timing data.").

used to iterate PNT profiles. This activity is fraught with complexity and should be undertaken with care and appropriate confidentiality, given the sensitivities involved. At a minimum, DHS should protect any testing activities under its Protected Critical Infrastructure Information ("PCII") Program, established under the Critical Infrastructure Information Act of 2002, to protect private sector infrastructure information voluntarily shared with the government.

V. CONCLUSION

CTIA looks forward to collaborating with NIST on a flexible, risk-based PNT profile. The profile should take into account industry contributions and the government's existing efforts to ensure service continuity and resilient systems.

Respectfully submitted,

/s/ Melanie K. Tiano
Melanie K. Tiano
Director, Cybersecurity and Privacy

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200
www.ctia.org

July 13, 2020