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

In the Matter of	)	Cybersecurity Profile for the
	)	Responsible Use of Positioning,
	)	Navigation and Timing (PNT)
Draft NISTIR 8323	)	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

November 23, 2020

Table of Contents

I. INTRODUCTION AND SUMMARY

CTIA[1] is pleased to issue these responsive comments to the National Institute of Standards and Technology's ("NIST") draft of NISTIR 8323: *Cybersecurity Profile for the Responsible Use of Positioning, Navigation and Timing (PNT) Services* ("Draft NISTIR 8323" or "the Draft Profile").[2] PNT services are incredibly important, fueling critical infrastructure, everyday business operations, and consumer applications—all of which benefit society. CTIA is encouraged by NIST's application of the flexible and risk-based Cybersecurity Framework to PNT services in Draft NISTIR 8323. Doing so imbues Draft NISTIR 8323 with many of the features that made the Cybersecurity Framework a success.

CTIA encourages NIST to take three important steps as it finalizes Draft NISTIR 8323. *First*, NIST should make explicit that private-sector use of the Draft Profile is voluntary. *Second*, NIST should actively collaborate with the private sector in order to draw more heavily from private-sector standards and best practices for securing PNT services. CTIA and the telecom sector have been pleased to work with NIST on this and will continue to do so. *Third*, NIST should ensure that the Draft Profile retains its flexible and outcome-based approach, particularly if NISTIR 8323 will inform other federal workstreams or federal procurement.

---

[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] *See Draft NISTIR 8323: Cybersecurity Profile for the Responsible Use of Positioning, Navigation and Timing (PNT) Services*, NIST (Oct. 2020), https://csrc.nist.gov/publications/detail/nistir/8323/draft ("*Draft NISTIR 8323*").

II. INDUSTRY—PARTICULARLY THE WIRELESS INDUSTRY—UTILIZES PNT TO DELIVER ENORMOUS BENEFITS TO CONSUMERS, WHILE KEEPING SECURITY AT THE FORE.

A. PNT Services Facilitate Innovative Services that Ultimately Benefit Consumers.

The Communications Sector uses PNT services for myriad critical functions. As the government has recognized, the Communications Sector performs "enabling functions . . . across all critical infrastructure sectors."[3] As the President explained in his Executive Order on PNT services ("PNT Executive Order"), "[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, all modes of transportation, precision agriculture, weather forecasting, and emergency response."[4] Indeed, communications networks are important for a host of PNT services that facilitate public safety and disaster relief.[5]

In addition to critical infrastructure applications, PNT services facilitate innovative consumer-enhancing services. PNT services deliver precise time data—"within 100 billionths of a second"—from satellites equipped with atomic clocks.[6] This data "is crucial to a variety of economic activities around the world," such as those undertaken by financial institutions, which utilize "precise time [data] for setting internal clocks used to create financial transaction timestamps."[7] Widespread GPS functionality in mobile devices has made navigation of foreign

---

[3] White House, Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (Feb. 12, 2013), https://www.govinfo.gov/content/pkg/DCPD-201300092/html/DCPD-201300092.htm.

[4] Exec. Order No. 13905, 85 Fed. Reg. 9359, § 1 (Feb. 12, 2020) ("*PNT Executive Order*").

[5] *Safety*, GPS.gov, https://www.gps.gov/applications/safety/ (last visited Nov. 19, 2020).

[6] *Timing*, GPS.gov, https://www.gps.gov/applications/timing/ (last visited Nov. 19, 2020).

[7] *Id.*

and unfamiliar locations anywhere in the world as easy as navigating one's own neighborhood.[8] GPS-enabled tools have freed consumers from "traditional problems" with outdoor recreation, such as hiking or fishing, like "getting lost in unfamiliar or unsafe territory."[9] Innovative PNT services have also offered entirely new forms of recreation, such as mobile applications in which users interact with real-world physical locations. Snapchat's "Snap Map" uses GPS functionality to allow users to interact with individuals, events, and businesses across the world.[10] Similarly, the "GPS-based game Pokémon Go" was downloaded by hundreds of millions of consumers.[11]

The incorporation of PNT services into Internet of Things ("IoT") applications promises to deliver unprecedented benefits. Businesses can embed "[l]ocation and tracking devices" to "track valuable assets such as cargo being shipped internationally."[12] Wildlife management groups use GPS-enabled IoT collars to track lions and cheetahs for longer periods of time and at much lower cost than traditional tracking collars.[13] This technology can also be used to save lives: health researchers have proposed a wearable bracelet that would use GPS tracking and

---

[8] *See* Joe Hindy, *10 best GPS apps and navigation apps for Android*, Android Authority (Sept. 3, 2020), https://www.androidauthority.com/best-gps-app-and-navigation-app-for-android-357870/ ("Most navigation apps act the same way. You input directions, follow them to your destination, and that's about it.").

[9] *See, e.g.*, *Recreation*, GPS.gov, https://www.gps.gov/applications/recreation/ (last visited Nov. 19, 2020).

[10] *See About Snap Map*, Snapchat, https://support.snapchat.com/en-US/a/snap-map-about (last visited Nov. 19, 2020).

[11] *See, e.g.*, Rachel Swatman, *Pokémon Go catches five new world records* (Aug. 10, 2016), https://www.guinnessworldrecords.com/news/2016/8/pokemon-go-catches-five-world-records-439327.

[12] *See GPS Applications in IoT (Internet of Things)*, Data Alliance, https://www.data-alliance.net/blog/gps-applications-in-iot-internet-of-things/ (last visited Nov. 19, 2020).

[13] Charles McLellan, *GPS collars for lions and cheetahs: How IoT and open source are protecting rare animals*, ZDNet (June 15, 2020, 11:03 A.M.), https://www.zdnet.com/article/gps-collars-for-lions-and-cheetahs-how-iot-and-open-source-are-protecting-rare-animals/.

advanced analytics to track the spread of COVID-19.[14]

B. Industry Uses Varied PNT Sources and Keeps PNT-Reliant Services Secure and Reliable.

Good security is good business. Disruption to PNT services can cause significant costs, delays, or degradation of functions and service. Accordingly, the wireless industry works tirelessly to protect its customers and networks from the enormous costs associated with the disruption or manipulation of PNT and has prioritized resiliency for interruptions that do occur.

The wireless industry uses varied techniques and technologies to secure networks and mitigate the risk of GPS outages. As CTIA detailed in previous comments, the wireless industry regularly manages PNT reliability and security, with rerouting, device-based navigation and timing capabilities, and cloud-based or software-based applications.[15] These technologies are deployed in varied ways across the different networks built and managed by carriers. Indeed, carriers regularly deal with PNT reliability, including outages. It is common for carriers to receive notifications from government of planned or ongoing PNT outages, and industry deals seamlessly with those events. Other security practices and mitigation strategies by carriers include vulnerability testing, ongoing threat monitoring, utilizing smart antenna technology to deny interfering signals access to receivers of PNT data, and detailed backup plans, redundancies, and contingency preparedness in case of an outage.[16]

The entire global ecosystem is investing in reliability and resiliency because timing and

---

[14] *See* Y. Weizman et al., *Use of wearable technology to enhance response to the Coronavirus (COVID-19) pandemic*, Public Health (July 1, 2020), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7328532/.

[15] *See* Comments of CTIA, Profile of Responsible Use of Positioning, Navigation, and Timing Services, Docket No. 200429 0124, at 6 (July 13, 2020), https://www.nist.gov/system/files/documents/2020/07/13/pnt-0024.pdf.

[16] *See id.* at 7–8.

synchronization will be critical to 5G and future innovation. Original equipment manufacturers ("OEMs") address PNT reliability in the design of network equipment and devices by, for example, including RF flexibility to accommodate multiple types of PNT services and GNSS receivers. Likewise, the 3rd Generation Partnership Project ("3GPP") is among groups looking at network needs and performance expectations related to positioning and timing.[17]

The wireless industry has access to PNT standards that facilitate the secure delivery of PNT services based on performance and outcome expectations. In April, for example, the Department of Defense ("DoD") 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]."[18] It sets specific "minimum performance standards for" an enumerated set of "performance parameter[s]."[19]

5G-fueled security improvements will continue to enhance the security of PNT. The wireless ecosystem is committed to ensuring the development of a secure and effective 5G deployment, with efforts from individual carriers, standards-setting bodies, and public-private partnerships with federal agencies.[20] The resulting improvements will bring substantial

---

[17] *See, e.g.*, Tracy Cozzens, *3GPP approves NaVIC for global commercial use*, GPS World (Oct. 24, 2019), https://www.gpsworld.com/3gpp-approves-navic-for-global-commercial-use/ ("Global mobile wireless standards body 3GPP has given its approval to the regional navigation system created by the Indian Space Research Organization (ISRO), known as NaVIC . . . . The approval was given for the system's use in Rel-16 LTE and Rel-17 5G NR specifications, paving the way for wider commercial adoption of NaVIC and allowing it to be integrated with 4G, 5G and internet of things technology (IoT)."); *see also infra* Section V.

[18] *5th Ed. of the GPS Standard Position Service Performance Standard*, DoD, at Foreword (Apr. 2020), https://www.gps.gov/technical/ps/2020-SPS-performance-standard.pdf.

[19] *Id.* at 35.

[20] *See Managing Security Risk in the Transition to 5G, Report on Risks to 5G From Legacy Vulnerabilities and Best Practices for Migration*, CSRIC Working Group 2 (June 2020), https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-

enhancements to the ecosystem, including PNT. 5G will facilitate faster and more effective security—from individual devices, through to network slicing and software defined networks that improve redundancy and recovery. 5G products will also be capable of receiving PNT services from multiple constellations, from GPS to Galileo and hybrid options.[21]

III. DRAFT NISTIR 8323 BEARS MANY OF THE HALLMARKS OF AN EFFECTIVE NIST PUBLICATION.

A. The Draft Profile Delivers Valuable Guidance by Applying the Cybersecurity Framework to PNT Services.

The Draft Profile "is based on the Cybersecurity Framework"[22] and "supports and is informed by cybersecurity risk management processes."[23] Indeed, the basic structure of the Draft Profile maps (i) the four implementation components from the PNT Executive Order, to (ii) the five functions—and their associated categories and subcategories—of the Cybersecurity Framework. The PNT Executive Order's four components are: "[1] identify systems, networks, and assets dependent on PNT services; [2] identify appropriate PNT services; [3] detect the disruption and manipulation of PNT services; and [4] manage the associated risks to the systems, networks, and assets dependent on PNT services."[24] The Cybersecurity Framework's Functions and Categories are summarized by the table below, which was excerpted from the Cybersecurity

---

interoperability-council-vii; *see also Protecting America's Next-Generation Networks*, CTIA (2018), https://api.ctia.org/wp-content/uploads/2018/07/ProtectingAmericasNetworks_FINAL.pdf.

[21] *See, e.g.*, *5G - a huge potential market for GNSS*, European Global Navigation Satellite Systems Agency (Oct. 31, 2019), https://www.gsa.europa.eu/newsroom/news/5g-huge-potential-market-gnss ("Thanks to its multi-constellation capacity (Galileo, GPS, BeiDou, and GLONASS), [a new 5G-enabled] receiver is ideal for global deployments and is unaffected by ionospheric errors, with automatic ionospheric correction.").

[22] *Draft NISTIR 8323*, at ii.

[23] *Id.* at 5.

[24] *See PNT Executive Order*, § 4(a).

Framework.[25]

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

As a result of this approach, the PNT Profile is effectively a series of tables that provide usable guidance for securing PNT systems within the rubric of the Cybersecurity Framework.[26]

---

[25] *See Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, at 23, NIST (Apr. 16, 2017), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf ("*Cybersecurity Framework*").

[26] *See Draft NISTIR 8323*, at 11–61.

This is prudent. By using the Cybersecurity Framework, Draft NISTIR 8323 delivers important security outcome expectations *from* the Executive Order *to* stakeholders using a format that is familiar to both the public and the private sectors. Indeed, as of last year, the Cybersecurity Framework had been downloaded more than half a million times.[27] And by applying the Cybersecurity Framework to PNT services, Draft NISTIR 8323 imported many of the features that made that Framework effective.

B. Draft NISTIR 8323 Contains Many Features that Made the Cybersecurity Framework a Success.

Draft NISTIR 8323 shares three of the features that made the Cybersecurity Framework successful: it is (1) flexible, (2) risk-based, and (3) the product of true collaboration. It is flexible. Draft NISTIR 8323 notes that "[t]he Profile provides a *starting point* from which organizations *can customize their approach* and develop the most appropriate processes to manage cybersecurity risk to their PNT services and data essential for the reliable and efficient behavior of critical infrastructure applications."[28] It explains that "[s]uccessful implementations require *a holistic approach rather than a checklist*."[29]

It is risk-based. The Draft Profile "supports and is informed by cybersecurity risk management processes."[30] Using the Draft NISTIR 8323, "organizations can make more informed decisions—based on business needs and risk assessments—to select and prioritize

---

[27] *See NIST Marks Fifth Anniversary of Popular Cybersecurity Framework*, NIST (Feb. 12, 2019), https://www.nist.gov/news-events/news/2019/02/nist-marks-fifth-anniversary-popular-cybersecurity-framework#:~:text=Interest%20in%20using%20the%20Cybersecurity,its%20initial%20publication%20in%202014.

[28] *Draft NISTIR 8323*, at 5 (emphasis added).

[29] *Id.* at 12 (emphasis added); *see also id.* at 1 ("The Profile is not intended to serve as a solution or compliance checklist[.]").

[30] *Id.* at 5.

cybersecurity activities and expenditures that help identify systems dependent on PNT, identify appropriate PNT sources, detect disturbances and manipulation of PNT services, manage the risk to these systems, and ensure resiliency."[31] Profile users are urged to "[e]valuate PNT services based on organizational requirements and risks."[32]

It is the result of collaboration. Draft NISTIR 8323 resulted from "an open and collaborative process involving public and private sector stakeholders."[33] The initial request for information generated 39 comments from diverse group of stakeholders, including the wireless industry.[34] NIST also held a Virtual Workshop on PNT Profile Development.[35] CTIA has met with NIST and looks forward to continuing to discuss approaches to PNT with NIST and the Department of Homeland Security ("DHS").

CTIA applauds NIST's adoption of these elements and encourages NIST to make explicit another element: voluntariness.

IV. CTIA URGES NIST TO MAKE EXPLICIT THAT PRIVATE-SECTOR USE OF NISTIR 8323 WILL BE VOLUNTARY.

The Draft Profile correctly recognizes that the Cybersecurity Framework was intended to offer "*voluntary* guidance[.]"[36] Indeed, as NIST Director Copan explained, the Cybersecurity

---

[31] *Id.*

[32] *Id.* at 22.

[33] News Release, NIST, Safeguarding Critical Infrastructure: NIST Releases Draft Cybersecurity Guidance, Develops GPS-Free Backup for Timing Systems, https://nist.gov/pnt (last visited Nov. 19, 2020).

[34] *See Comments Received for RFI on Profile of Responsible Use of Positioning, Navigation, and Timing Services*, NIST (updated July 15, 2020) https://www.nist.gov/itl/pnt/comments-received-rfi-profile-responsible-use-positioning-navigation-and-timing-services.

[35] *See NIST Profile on Responsible Use of PNT Services*, NIST Workshop (September 15-16, 2020), https://www.nist.gov/news-events/events/2020/09/nist-profile-responsible-use-pnt-services.

[36] *Draft NISTIR 8323*, at 5 (emphasis added); *see also Cybersecurity Framework*, at vi (describing the Cybersecurity Framework as a "voluntary Framework").

Framework has been successful, in part, because "[i]t is voluntary."[37] CTIA understands that the Draft Profile—as an application of the Cybersecurity Framework—is also voluntary. Nevertheless, CTIA urges NIST to make this fact explicit in the text of the Draft Profile.

This explicit clarification is needed in light of the structure of Draft NISTIR 8323. Specifically, the Draft Profile generally frames its subcategory applications to PNT in prescriptive terms. For example, it directs readers to, *inter alia*:

- "Establish and manage the identification and authentication credentials of PNT data sources and applications using PNT data."[38]
- "Schedule, perform, record, and review records of maintenance and repairs on PNT devices and components."[39]
- "Configure the PNT system to provide only essential capabilities."[40]

To be sure, this language is not problematic when placed in the context of the Profile working as intended, *i.e.*, as a voluntary, flexible document that empowers—but does not require—organizations to select the applications that are appropriate for their organization. However, this prescriptive language could lead stakeholders to (mistakenly) interpret the Draft Profile as a set of mandatory requirements. CTIA encourages NIST to include explicit and unambiguous language to explain that the Draft Profile is voluntary. CTIA suggests the following language at

---

[37] Walter Copan, Dir., NIST, Remarks at the Brookings Inst., Developing the NIST Privacy Framework: How Can a Collaborative Process Help Manage Privacy Risks?,at 10–11 (Sept. 24, 2018), https://www.brookings.edu/wp-content/uploads/2018/09/gs_20180924_nist_privacy_transcript.pdf; *see also* Donna Dodson, Chief Cybersecurity Advisor and Director of NCCoE, NIST, Testimony Before the Subcomm. on Oversight of the H. Comm. on Science, Space, & Technology, at 3 (Oct. 25, 2017), https://docs.house.gov/meetings/SY/SY21/20171025/106556/HHRG-115-SY21-Wstate-DodsonD-20171025.PDF ("The voluntary, risk-based, flexible, repeatable, and cost-effective approach of the Framework helps those who use the Framework to manage cybersecurity risk.").

[38] *Draft NISTIR 8323*, at 34.

[39] *Id.* at 40.

[40] *Id.* at 41.

the end of Section 1.3 (Audience): "The Profile is *voluntary* for the private sector. Private organizations are not required to implement the Draft Profile but may find it useful."

V. NIST'S ILLUSTRATIVE INFORMATIVE REFERENCES SHOULD INCORPORATE INDUSTRY-DRIVEN STANDARDS FROM CSRIC AND 3GPP, AND BE REGULARLY UDPATED.

NIST rightly includes private-sector informative references.[41] It can be difficult to identify the universe of potentially relevant documents and approaches, particularly where internal practices used by satellite and telecom carriers may not be captured in third-party documents. Carrier practices for managing network functions that rely on PNT are unique, sensitive, and proprietary, meaning that the solutions and mitigations are not likely to be widely available. As it identifies informative references, NIST should take care to avoid implying that the lack of third-party standards or guidance documents suggests a gap in actual security practices related to PNT.

NIST should draw heavily from industry-driven publications. The Federal Communications Commission's ("FCC") Communications Security, Reliability and Interoperability Council ("CSRIC"), led by wireless stakeholders, has identified technical, security, and cost issues, which can inform the management of cybersecurity risks to systems, networks, and assets that use PNT services.[42] The Alliance for Telecommunications Industry Solutions ("ATIS") also released a Technical Report detailing potential GPS vulnerabilities and issuing "general recommendations with the intent to reduce telecom industry and

[41] *See id.* at 65–66 (referencing, *inter alia*, IEEE and IETF standards).

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

communications sector susceptibility to [those] vulnerabilities."[43] Several papers have been generated to address particular aspects of PNT, such as synchronization in mobile networks. For example, *Rubidium Sync Holdover Ensures Mobile Service Availability* by Microsemi, informs "mobile network operators and their equipment suppliers of changes in synchronization requirements as networks advance. . . . In particular, it focuses on the need for superior holdover performance as sync specifications become more stringent and difficult to meet."[44]

NIST does not refer to 3GPP, but the work of 3GPP on 5G and future telecom specifications necessarily addresses synchronization and timing, including resiliency and security. PNT reliance is inherent in evolving 5G standards given the centrality of timing accuracy to future use cases and networks. Examples include: 3GPP Tdoc R2-1817172, *Overview of UE Time Synchronization Methods* (November 2018);[45] 3GPP TS 22.104, *Service requirements for cyber-physical control applications in vertical domains* (March 2019);[46] and generally the work of SA WG1, which includes a *Feasibility Study on 5G Timing Resiliency*

---

[43] *See generally GPS Vulnerability, ATIS-0900005*, ATIS (Sept. 7, 2017), https://access.atis.org/apps/group_public/download.php/36304/ATIS-0900005.pdf. ATIS has remained deeply involved in PNT security. *See, e.g.*, *Presentation from ATIS Time & Money Conference*, GPS.gov (Jan. 28, 2020), https://www.gps.gov/multimedia/presentations/2020/ATIS/ (presentation from ATIS that "provides an overview of threats to GPS/PNT and suggests methods for protecting the financial services sector against PNT spoofing."); *Timing Security: Mitigating Threats in a Changing Landscape Webinar*, ATIS (May 22, 2018), https://www.atis.org/wp-content/uploads/01_news_events/webinar-pptslides/Timing-Security5222018.pdf; Letter from ATIS to NIST on PNT RFI Response (July 13, 2020) https://www.nist.gov/system/files/documents/2020/07/13/pnt-0022.pdf.

[44] *See Rubidium Sync Holdover Ensures Mobile Service Availability*, at 1, Microsemi (2014), https://www.microsemi.com/document-portal/doc_download/134355-rubidium-sync-holdover-ensures-mobile-service-availability.

[45] *GPP Tdoc R2-1817172: Overview of UE Time Synchronization Methods*, 3GPP (Nov. 2018), https://www.3gpp.org/ftp/TSG_RAN/WG2_RL2/TSGR2_104/Docs/R2-1817172.zip.

[46] *3GPP TS 22.104, Service reequipments for cyber-physical control applications in vertical domains*, 3GPP (Mar. 29, 2020), https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3528.

System (September 2020). [47] 3GPP has recognized that 5G "also brings positioning enhancements, meaning it can gradually evolve towards a full alternative solution for GNSS, e.g., offer both timing and positioning service, and/or work in concert with other land-based positioning services."[48] Importantly there are many use cases for 5G which may require diverse treatment by SSAs in the future, so NIST should work to ensure its profile can accommodate these applications, and be adapted. As SA WG1 said "SA1 Release-17 studies have identified synchronization requirements associated to specific verticals . . . . As an example, the listed time synchronization requirements for Audio-Visual Service Production in TR 22.827, Future Railway Mobile Communication System in TR 22.889, and Communication Services for Critical Medical Applications in TR 22.826 focus on the time synchronization accuracy among the devices connected and the synchronized video and audio information."[49] Work toward Release 18 likewise addresses PNT, as in 3GPP TR 22.878 V0.1.0, *Feasibility Study on 5G Timing Resiliency System* (September 2020)which "identifies additional potential requirements on the 5G system to support time-synchronization services in public and vertical domains, including both the ability to improve resiliency of timing services involving technologies supported by 5G and the ability to the ability to act as a backup for GNSS timing services."[50] There are myriad complexities surrounding PNT, but private sector experts in 3GPP and elsewhere are addressing them.

---

[47] 3GPP TSG SA Meeting # 88e, *SP-200573, Feasibility Study on 5G Timing Resiliency System*, Acronym: FS_5TRS, Unique identifier: 880037 (June 30th – July 3rd 2020), https://portal.3gpp.org/Home.aspx#/meeting?MtgId=38165.

[48] *Id.*

[49] *Id.*

[50] *3GPP TR 22.878, Feasibility Study on 5G Timing Resiliency System*, 3GPP (Sept. 2020), https://portal.3gpp.org/ngppapp/CreateTdoc.aspx?mode=view&contributionUid=S1-203386#.

NIST should ensure that its guidance is updated regularly to keep up with evolving practices and with other NIST documents from which NISTIR 8323 draws. For example, the Draft Profile refers to NIST SP 800-53 Rev. 4 throughout the document,[51] but SP 800-53 recently underwent a significant update with the promulgation of Rev. 5.[52]

VI. NIST SHOULD EXPLAIN HOW THE DRAFT PROFILE WILL INTERACT WITH OTHER FEDERAL WORKFLOWS AND PROMOTE FLEXIBLE INTEGRATION IN FEDERAL PROCUREMENT.

NIST should address how the Draft Profile will influence—or interact with—other federal workstreams. There is a good deal of activity across government on PNT and related issues. DHS's Cybersecurity and Infrastructure Security Agency ("CISA") and others have examined "civil PNT" concerns, while DoD has been looking at military issues, as reflected in CISA's April 2020 report on PNT.[53] Recently, in October 2020, the U.S. Army identified an office for PNT Modernization.[54]

NIST should also maintain the flexible approach currently embodied by Draft NISTIR 8323, given the document's potential for interaction with other federal workstreams and use in federal procurement. The PNT Executive Order envisions that NISTIR 8323 will eventually be used by federal government procurement officers in selecting vendors that provide and rely on

---

[51] *See Draft NISTIR 8323*, at 14–61.

[52] *See generally NIST Special Publication 800-53, Revision 5: Security and Privacy Controls for Information Systems and Organizations*, NIST (Sept. 2020), https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

[53] *See generally Report on Positioning, Navigation, and Timing (PNT) Backup and Complementary Capabilities to the Global Positioning System (GPS)*, DHS CISA (Apr. 8, 2020), https://www.cisa.gov/sites/default/files/publications/report-on-pnt-backup-complementary-capabilities-to-gps_508.pdf.

[54] Nathan Strout, *US Army launching new PNT Modernization Office and Open Innovation Lab*, C4ISRNET (Sept. 10, 2020), https://www.c4isrnet.com/battlefield-tech/2020/09/10/army-launching-new-pnt-modernization-office-and-open-innovation-lab/.

PNT services. In particular, section 4(d) of the PNT Executive Order instructs the Secretary of Homeland Security to 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."[55] It is not clear what this will mean, but DHS may play an important role with other sector-specific agencies.

Accordingly, it is critical that NIST maintain the flexible, outcome-based approach to PNT security in Draft NISTIR 8323. As explained, PNT services support a diverse array of critical infrastructure, business operations, and consumer-facing services. Indeed, Draft NISTIR 8323 acknowledges the "broad and varied stakeholder community using PNT services."[56] This diversity of use cases precludes the development of one-size-fits-all procurement standards. CTIA thus urges NIST to maintain the Draft Profile's function as "*a flexible tool that can be used in diverse ways* by an organization to help meet mission and business objectives that are dependent upon the use of PNT services."[57]

VII. CONCLUSION

CTIA applauds NIST's efforts on NISTIR 8323. As this project advances, CTIA urges NIST to (1) make explicit the voluntary application of the Draft Profile to the private sector, (2) draw upon private sector expertise and experience in securing PNT services, and (3) clarify how the Draft Profile may be used relative to other federal PNT efforts—including procurement—and maintain a flexible, outcome-based approach to accommodate these workstreams.

---

[55] *PNT Executive Order*, § 4(d).

[56] *See Draft NISTIR 8323*, at ii.

[57] *Id.* at 4 (emphasis added).

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

November 23, 2020