Before the
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Gaithersburg, MD 20899

In the Matter of	)	
	)	
Profile of Responsible Use of Positioning, Navigation, and Timing Services	)	Docket No. 200429-0124
	)	

COMMENTS OF THE GPS INNOVATION ALLIANCE

The GPS Innovation Alliance ("GPSIA") submits these comments in response to the Notice and Request for Information ("RFI") issued by the National Institute of Standards and Technology ("NIST") in the above-referenced proceeding.[1/] The RFI seeks input on public and private sector use of positioning, navigation, and timing ("PNT") services, and standards, practices, and technologies used to manage cybersecurity risks to systems, networks, and assets dependent on PNT services. The GPSIA welcomes NIST's efforts to conduct this analysis. Because PNT functions demand a high degree of accuracy and resiliency, the U.S. Global Positioning System ("GPS") has been, and continues to be, the best technology to support a broad range of PNT functions. GPS will continue to be the gold standard for PNT functions through continued development of solutions to support resiliency and address disruptions and security risks, backstopped by strong Federal government enforcement against potential threats to GPS services.

I. INTRODUCTION

The GPSIA was formed in February 2013 to protect, promote, and enhance use of GPS and Global Navigation Satellite Systems ("GNSS") technologies. Members and affiliates of the GPSIA are drawn from a wide variety of fields and businesses reliant on GPS, including

---

1/ *See Profile of Responsible Use of Positioning, Navigation, and Timing Services,* Notice; Request for Information, 85 Fed. Reg. 31,743 (May 27, 2020) ("*RFI*").

manufacturing, aviation, agriculture, construction, defense, transportation, first responders, surveying, and mapping. The GPSIA also includes organizations representing consumers who depend on GPS for boating and other outdoor activities, and in their automobiles, smart phones, and tablets. The GPSIA recognizes the ever-increasing importance of GPS and other GNSS technologies to the global economy and infrastructure and is firmly committed to furthering GPS innovation, creativity, and entrepreneurship.

The RFI builds on Executive Order 13905,[2/] which recognizes the critical economic and societal benefits of GPS and other GNSS technologies for the delivery of PNT functions and the need to protect the national and economic security of the United States from disruptions to PNT services. The RFI represents a crucial next step to implement the Executive Order by examining how to maintain the security, robustness, and redundancy of PNT capabilities. The GPSIA is therefore pleased to submit these comments and answer questions about uses of PNT services and standards, practices, and technologies used to manage cybersecurity risks.

II. COMMENTS

A. The Public and Private Sector Depend on GPS for PNT Services.

The RFI asks commenting parties to describe any public or private sector need for and/or dependency on the use of PNT or any combination of these services.[3/] The public and private sectors rely heavily on PNT services, and GPS is the preeminent technology to provide them. As a critical national asset, GPS is used for PNT services by myriad industries in the commercial sector, including the aviation, agriculture, automotive, construction, electricity, finance, public

---

2/ *See Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services*, Executive Order 13905, 85 Fed. Reg. 9359 (Feb. 12, 2020). The GPSIA has expressed support for the Executive Order. *See* GPSIA Press Release, *GPS Innovation Alliance Welcomes Executive Order on PNT* (Feb. 12, 2020), https://www.gpsalliance.org/executive-order-on-pnt.

3/ *See RFI* at 31,745 (Question 1).

safety, and transportation industries. GPS is also critical to the burgeoning unmanned aerial vehicle and driverless car industries. More importantly, GPS is utilized by the Federal government in vital military and other applications that rely on a high degree of accuracy and resiliency. GPS receivers can be found in countless public and private sector devices, including in mobile phones, automobiles, airplanes, tractors, boats, and high-precision surveying equipment. Recent reports estimate that there are approximately 900 million GPS receivers in use in the U.S. today and 3 billion GPS receivers in the marketplace globally.[4/]

The proliferation and benefits of GPS devices have resulted in numerous gains in the U.S. economy. Since it was made available for civilian and commercial use nearly four decades ago, the economic value of GPS has been estimated to be $1.4 trillion.[5/] In the past decade alone, GPS applications have helped generate more than $1.2 trillion for the U.S. economy and millions of jobs. A disruption resulting in a loss of GPS service has been estimated to have a $1 billion per-day impact on the U.S. economy.[6/] In addition, there are more than 3.3 million jobs that rely on GPS technology, including approximately 130,000 jobs in GPS manufacturing industries and 3.2 million in the downstream commercial GPS-intensive industries.[7/] Those benefits are expected to grow. By 2025, the GPS market is estimated to reach $128.7 billion.[8/] More

---

[4/] *See* National Space-Based Positioning, Navigation, and Timing Advisory Board, *Twenty-Fourth Meeting*, at 14 (Nov. 2019), https://www.gps.gov/governance/advisory/meetings/2019-11/minutes.pdf; J. David Grossman, *Freedom to Innovate Promotes GPS Resiliency*, GPS WORLD (Aug. 1, 2019), https://www.gpsworld.com/freedom-to-innovate-promotes-gps-resiliency/.

[5/] *See* RTI International, *Economic Benefits of the Global Positioning System (GPS)*, at ES-1 (June 2019) ("RTI Study"), https://www.rti.org/sites/default/files/gps_finalreport.pdf.

[6/] *See* RTI Study at ES-4.

[7/] *See* Nam D. Pham, Ph.D., *The Economic Benefits of Commercial GPS Use in the U.S. and the Costs of Potential Disruption*, at 1 (June 2011), https://static1.squarespace.com/static/52850a5ce4b0683 94a270176/t/52d84e86e4b042903508ec47/1389907590034/GPS+Report+June+21+2011.pdf.

[8/] *See* KBV Research, *Global GPS (Global Positioning Systems) Market* (Nov. 2019), https://www.kbvresearch.com/global-positioning-systems-market/.

broadly, the Space-based Communications and Geospatial Intelligence segments, which include GPS, offer the potential to generate over $1 trillion in equity value over the next decade.[9/]

B. GPS Offers Highly Resilient PNT Services.

The RFI requests that commenters identify and describe any impacts to public or private sector operations if PNT services are disrupted or manipulated.[10/] Resiliency is among the core attributes that has made GPS essential for delivering PNT functions to the public and private sectors. As a multi-use asset, supporting both the day-to-day activities of consumers as well as the missions of our armed forces, GPS satellites have been built to meet the highest level of resiliency and redundancy requirements. GPS III satellites have a 15-year design life with greater accuracy and greater military power for anti-jamming operations. In addition, newer GPS devices have the ability to access multiple GNSS systems. Similarly, GPS-enabled timing devices employ high-stability oscillators to improve holdover performance – preserving the timing function of these devices in the unlikely event that GPS signals may be unavailable. Many GPS navigation devices also include resilient features like inertial navigation and map-matching algorithms to ensure that the position and navigation information they provide is sufficiently accurate to support a full range of functions. The most robust GPS receivers are augmented with either Inertial Measurement Units that propagate the PNT solution during GPS

9/ *See* Space Capital and Silicon Valley Bank, *The GPS Playbook*, at 18 (Mar. 2020), https://www.svb.com/contentassets/c0e37e68e9894f5a9719b0dacadb1aaf/the-gps-playbook-svb-2020.pdf.

10/ *See RFI* at 31,745 (Question 2).

outages or antenna electronics processors to steer antenna beams to GPS satellites as well as create nulls to block jammers.

Successive generations of GPS satellites have added accuracy, signal strength, and quality improvements and capabilities that bolster resiliency. For example, GPS satellites now provide on-board clock monitoring and enhanced jam-resistance functions. One of the most significant modernization efforts to GPS satellites to improve performance and resiliency includes the launch of the GPS III series of satellites built by Lockheed Martin. In addition to providing three times greater accuracy, those satellites will include up to eight times improved anti-jamming capabilities over any previous GPS satellites in the constellation, making them the most powerful and resilient GPS satellite ever put in orbit.[11/] The GPS III satellites will also provide improved accuracy, reliability, and interoperability with the new unique fourth civil signal known as the L1C signal, which is shared by other international GNSS systems, like Galileo. This modernization effort will not only benefit military users, but also improve future connectivity worldwide for civilian users that depend on GPS operations.

Nevertheless, like any radiofrequency-based system, whether satellite or terrestrial wireless, GPS is susceptible to both natural and man-made threats. And these threats can occur notwithstanding the existing safeguards that have been put in place by the Federal government, as discussed below. That is why the GPS industry recognizes that it is in the public interest to explore innovative complementary solutions. But those solutions must be fully evaluated to ensure that they offer robust and reasonably equivalent capabilities and a level of performance on

---

[11/] *See* Lockheed Martin News Release, *Third Lockheed Martin-Built GPS III Satellite Delivered to Cape Canaveral for First U.S. Space Force GPS III Launch in April* (Feb. 10, 2020), https://news.lockheedmartin.com/2020-02-10-Third-Lockheed-Martin-Built-GPS-III-Satellite-Delivered-to-Cape-Canaveral-for-First-U-S-Space-Force-GPS-III-Launch-in-April.

par with GPS technologies. The Department of Transportation is currently examining proposed solutions and conducting demonstrations of various backup options.[12/] GPSIA supports those efforts.[13/] However, as pointed out previously, complementary solutions require considerable development over time to ensure they reach their maximum potential as true PNT complements to GPS. Therefore, the Federal government must ensure that its resources continue to be principally directed to maintaining and improving the existing GPS system.

C. Security Risks to GPS Should be Managed on a Case-By-Case Basis.

The RFI asks commenters to identify approaches to managing cybersecurity risks and the risk of disruption or manipulation of PNT services.[14/] Each GPS-enabled application has unique requirements driven by its intended function, environment, and design factors. For example, a GPS receiver used for synchronizing financial transactions has different demands than a GPS receiver found in an autonomous vehicle. The former focuses on timing while the latter requires precise positioning to help maintain lane-level guidance. Similarly, high-precision surveying equipment capable of delivering centimeter-level accuracy has different receiver and antenna requirements than those found in a typical smartphone, which requires less exacting location accuracy. And the requirements for a military GPS receiver, which could require positional accuracy by fractions of a second for mission-critical operations, are much more demanding than those for the receiver in a commercial Internet of Things device that reports its position hourly or daily. Accordingly, approaches to managing security risks and disruptions to GPS devices are,

---

12/ *See U.S. Department of Transportation, Demonstration of Backup and Complementary Positioning, Navigation, and Timing (PNT) Capabilities of Global Positioning System (GPS),* Request for Information, 84 Fed. Reg. 19,154 (May 3, 2019).

13/ *See* Comments of the GPS Innovation Alliance, Docket No. DOT-OST-2019-0051 (filed June 3, 2019).

14/ *See RFI* at 31,745 (Questions 4 and 6).

and should continue to be, tailored to the intended function, environment, and design factors of those devices.

Today's regulatory landscape correctly recognizes the requirement for different approaches to managing risks. Not only does the ability to mitigate and address risks based on the specific needs of a GPS application best ensure that the wide variety of GPS services remain robust and secure, but it also promotes innovation in developing techniques for increasing resiliency. For example, the flexibility to innovate has allowed many receivers, as noted above, to be designed to be capable of receiving signals from multiple GNSS systems. The Federal government must recognize that there is no one-size-fits-all solution to GPS resiliency and avoid technology mandates or standards setting.

To the contrary, technology mandates, in addition to stifling innovation, are often ineffective at addressing disruptions to GPS services. For example, a technology mandate would have no impact or ability to stop a malicious actor intent on illegally interfering with GPS or another wireless technology through jamming or spoofing. Only vigorous enforcement of U.S. Federal law by the Federal Communications Commission ("FCC") and other government agencies – which already prohibit the manufacture, importation, marketing, sale, and operation of GPS (and other wireless service) jammers – can keep these illegal devices out of the hands of those seeking to disrupt GPS operations. The Federal government should continue to support and further enhance those efforts and enforcement tools.

D. The Public and Private Sectors Routinely Work Together to Respond to and Resolve GPS Disruptions.

The RFI asks commenting parties to identify and describe any approaches, practices, and/or technologies used by the public or private sector to recover or respond to PNT

disruptions.[15/] Both the public and private sectors have implemented several techniques and approaches to respond to and recover from PNT disruptions. For example, the FCC provides consumer alerts, with the ability for individuals to file complaints about unlawful jamming, and employs several field offices to investigate complaints of interference to GPS operations.[16/] And the agency imposes significant fines on those that are found to have willfully and repeatedly interfered with GPS signals.[17/]

Similarly, the U.S. Coast Guard makes available a public website for consumers to report GPS service degradations, disruptions, and other incidents or anomalies.[18/] The website includes information from those reports along with input from interagency partners and the most likely cause of the reports.[19/] In addition, the Department of Homeland Security ("DHS") has invested considerable resources into cataloging observed and potential spoofing scenarios and hosts events to assess GPS vulnerabilities in critical infrastructure and increase resiliency.[20/] Through

---

15/ *See RFI* at 31,745 (Question 7).

16/ *See* FCC, Jammer Enforcement, https://www.fcc.gov/general/jammer-enforcement (last visited July 7, 2020); *see, e.g.*, Notice of Unlicensed Operation and Notification of Harmful Interference from David C. Dombroswki, Regional Director, Region One, Enforcement Bureau, FCC, to Frank Reimer, East Brunswick, New Jersey (Apr. 11, 2019) (explaining that agents from the New York Office of the FCC's Enforcement Bureau investigated a complaint from the Federal Aviation Administration alleging that spurious emissions on the frequency 1575.42 MHz were routinely causing harmful interference to its GPS receivers at the Newark Airport).

17/ *See, e.g.*, *Gary P. Bojczak, Whitehouse Station, New Jersey*, Notice of Apparent Liability, 28 FCC Rcd 11589 (2013) (imposing a forfeiture of $31,875 against an individual for operating a GPS jammer that caused harmful interference to a ground-based augmentation system operated by the Port Authority of New York and New Jersey and designed to increase the precision of GPS-based navigation at Newark Liberty International Airport, one of the busiest airports in the country).

18/ *See* U.S. Department of Homeland Security, United States Coast Guard, GPS Problem Reporting, https://navcen.uscg.gov/?pageName=gpsUserInput (last visited July 7, 2020).

19/ *See* U.S. Department of Homeland Security, United States Coast Guard, GPS Problem Reports Status, https://navcen.uscg.gov/?Do=GPSReportStatus (last visited July 7, 2020). As indicated in those reports, the majority of the causes are listed as problems with individual user equipment rather than issues with the GPS constellation itself, which remains robust.

20/ *See, e.g.*, U.S. Department of Homeland Security, 2020 GPS Equipment Testing for Critical Infrastructure, https://beta.sam.gov/opp/1942578638c542239fc04851f252f6f6/view (last visited July 7,

their participation in these events, GPS manufacturers can evaluate jamming and spoofing attacks and develop industry solutions that are tailored to address and prevent those threats. DHS also maintains best practices for improved robustness of time and frequency sources, including GPS, in fixed infrastructure locations and a cybersecurity strategy to reduce vulnerabilities and build resilience.[21/] More recently, DHS proposed a framework for PNT resiliency, which classifies mitigation approaches into tiers such as using integrated solutions, improved technologies, and increased education to improve resiliency.[22/]

These joint efforts by the public sector and private industry, among others, have been instrumental in preserving the PNT functions of GPS and ensuring that when disruptions occur they are promptly addressed.

III. CONCLUSION

GPSIA appreciates the efforts that NIST has taken and will take to evaluate systems, networks, and assets dependent on PNT services and to identify mechanisms to detect and mitigate against security risks. In conducting this evaluation and developing a PNT profile, NIST should recognize and continue to support the important PNT functions that GPS provides and only pursue alternatives that can serve as appropriate complements to the high-level and irreplaceable function that GPS serves.

2020); *see also* Tracy Cozzens, *DHS to Host 2020 GPS Equipment Testing Event This Summer*, GPS WORLD (Apr. 29, 2020), https://www.gpsworld.com/dhs-to-host-2020-gps-equipment-testing-event-this-summer/.

[21/] *See* U.S. Department of Homeland Security, *Best Practices for Improved Robustness of Time and Frequency Sources in Fixed Locations* (Jan. 6, 2015), https://www.dhs.gov/sites/default/files/publications/GPS-PNT-Best-Practices-Time-Frequency-Sources-Fixed-Locations-508.pdf; *U.S. Department of Homeland Security Cybersecurity Strategy* (May 15, 2018), https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf.

[22/] *See* U.S. Department of Homeland Security, *PNT Program & Conformance Framework*, at 3 (Nov. 20, 2019), https://www.gps.gov/governance/advisory/meetings/2019-11/wong-villee.pdf.

Respectfully submitted,

/s/ J. David Grossman

J. David Grossman
Executive Director
GPS Innovation Alliance
1800 M Street, NW
Suite 800N
Washington, DC 20036
202-628-9586

July 13, 2020