GPS Innovation Alliance

November 23, 2020

Mr. James McCarthy
Applied Cybersecurity Division, Information Technology Laboratory
National Institute of Standards and Technology
100 Bureau Drive, Mail Stop 2000
Gaithersburg, MD 20899

Dear Mr. McCarthy:

The GPS Innovation Alliance ("GPSIA") appreciates the continued work of the National Institute of Standards and Technology ("NIST") to evaluate systems, networks, and assets dependent on positioning, navigation, and timing ("PNT") services and to identify mechanisms to detect and mitigate against security risks.

GPS, as the gold standard for PNT services, is vital to our national and economic security and relied upon by a myriad of industries, including aviation, agriculture, automotive, construction, electricity, finance, public safety, and transportation. These applications have come to depend on GPS because of its ability to provide a high degree of accuracy and resiliency.

Recognizing the ever-increasing importance of GPS and other PNT services to the global economy and critical infrastructure, the draft PNT cybersecurity profile offers an important roadmap for organizations dependent on these services. GPSIA supports the development of the PNT cybersecurity profile and is pleased to provide the following comments:

- In recent years, GPS manufacturers and applications developers have added new and innovative techniques for increasing resilience, including designing receivers capable of receiving signals from multiple satellite-based constellations. Multi-constellation GNSS provides an additional form of redundancy for systems dependent on GPS and may be considered a means for achieving some of the objectives of the PNT cybersecurity profile.

- The Department of Homeland Security ("DHS") has hosted test events, where infrastructure owners and operators and GPS receiver manufacturers can test their equipment against GNSS spoofing scenarios. GPSIA would urge NIST to include a recommendation that infrastructure owners and operators utilize the DHS testing process on a voluntary basis as another source for threat information.

- NIST should ensure that the voluntary recommendations included in the PNT cybersecurity profile are consistent with the Commerce Control List (CCL) as well as the International Traffic in Arms Regulations (ITAR) controls on GPS/GNSS receivers. This can ensure responsible growth and development of GPS/GNSS technology, applications and markets while safeguarding U.S. national security interests.

- GPS/GNSS receivers are used by the majority of the 16 DHS-defined critical infrastructure sectors, including communications networks, financial systems and the electric grid, but not all GPS/GNSS devices and applications within these sectors are necessarily critical infrastructure. A one-size-fits-all approach, even within a given sector, will not work. Therefore, it is important that the PNT cybersecurity profile avoid prescriptive requirements, and allow for flexibility based on the intended function, environment, and design factors of the GPS/GNSS receiver.

- GPSIA supports the structure of the overall NIST cybersecurity framework and believes that it serves as a successful model for organizations, including infrastructure owners and operators who are dependent on PNT services.

Thank you again for the opportunity to share our industry's perspective. GPSIA looks forward to working with NIST and other stakeholders in support of solutions to promote resiliency and address disruptions and security risks, backstopped by strong Federal government enforcement against potential threats to GPS service.

Sincerely,

David Grossman

J. David Grossman
Executive Director
GPS Innovation Alliance