July 13, 2020

**VIA ELECTRONIC FILING**

National Institute of Standards and Technology
U.S. Department of Commerce
100 Bureau Drive
Gaithersburg, MD 20899

**RE: Request for Information on Responsible Use of Positioning, Navigation, and Timing Services**

To Whom It May Concern:

The Alliance for Automotive Innovation ("Auto Innovators") appreciates the opportunity to submit these comments in response to the Request for Information (RFI) about public and private sector use of positioning, navigation, and timing (PNT) services.

As noted in Executive Order 13905, *Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services*, PNT services are playing an increasingly vital role in transportation. For example, modern vehicles are incorporating more functions and features that are dependent on PNT services. Since disruption or manipulation of these services may undermine these features and functions, the reliability and resilience of PNT services is of growing importance to the automotive industry.

To that end, Auto Innovators supports ongoing efforts to enable public and private sectors - including the automotive sector - to identify systems, networks, and assets dependent on PNT services, to detect the disruption and manipulation of PNT services, and to manage the associated cybersecurity risks to the systems, networks, and assets dependent on PNT services.

The following is Auto Innovators' reply to the numbered questions in the RFI.

1. **Describe any public or private sector need for and/or dependency on the use of positioning, navigation, and timing, or any combination of these, services.**

New and emerging automotive technologies are increasingly dependent on PNT services. PNT services support embedded navigation and mapping features in vehicles, including route optimization, real-time traffic information, and the identification of points of interest. PNT services also facilitate location-based connected services for drivers and passengers, including parking location reminders, geofencing applications for teenage drivers, real-time weather and road condition information, and stolen vehicle location features.

In addition, PNT services enable technologies that can link third party service providers with a customer's vehicle. This includes services that dispatch emergency responders to the scene of a traffic collision, guide roadside assistance providers to a disabled vehicle on the road, or enable mobile fuel or

in-car delivery. PNT services are also increasingly important for connecting consumers with mobility services, such as carsharing, peer-to-peer ridesharing, or on-demand ride services.

PNT services may also play a role in vehicle maintenance. For example, the vehicle suspension system can be dynamically adjusted for known obstacles - such as speed bumps and potholes - based on signals from space-based PNT. The date, which can be derived from Global Navigation Satellite System (GNSS) signals, may be used to remind the driver of scheduled maintenance. Accumulated driving miles derived from GNSS signals can be used to notify the driver that it is time to rotate the tires or change the oil. Precise time alignment between electronic control units on the vehicle and offboard infrastructure can help support over-the-air software reprogramming.

Perhaps most critical, however, is the essential nature of PNT services to next-generation safety technologies. For example, GNSS signals can be used to supplement wheel odometry and inertial measurements to detect and control sideslip and skidding through selective braking. The active safety features on advanced Level 2 and Level 3 automated vehicles can use precise GNSS to identify the lane on the road the vehicle occupies. Level 4 autonomous vehicles can use GNSS signals to supplement perception information from external sensors (including cameras, LIDAR, and radar) to precisely localize the vehicle to a map. Level 4 automated vehicles also use Coordinated Universal Time (UTC) derived from GNSS for on-board sensor synchronization. In addition, vehicle-to-vehicle communication requires space-based PNT technology to derive vehicle location and to affix a timestamp to the core Basic Safety Message.

**2. Identify and describe any impacts to public or private sector operations if PNT services are disrupted or manipulated.**

Space-based PNT is vulnerable to disruption from jamming and spoofing. Both jamming and spoofing disruptions can impact vehicle functions that rely on PNT.

Jamming, whether intentional or unintentional, occurs when in-band noise overwhelms the GNSS tracking loops and renders satellite tracking impossible. Moderate jamming can degrade GNSS signal levels within a vehicle's receiver, which can compromise accuracy or provide gaps in PNT availability. Heavy jamming can prevent the vehicle from obtaining any time and location information.

Spoofing is always deliberate and involves the creation of false GNSS signals to attempt to fool the target receiver. Spoofing requires knowledge of the victim's location, trajectory, and speed. It requires the attacker to place sophisticated equipment in the vicinity of the victim, and to maintain this proximity while attempting to manipulate the victim's receiver.

GNSS is rarely used exclusively for vehicle localization, so the impacts of a spoofing attack may be mitigated. In vehicles, GNSS signals are commonly combined with measurements from local inertial measurement units (IMUs), such as gyroscopes and accelerometers. Automated and autonomous vehicles also combine GNSS/IMU measurements with perception sensors, such as cameras, LIDAR, radar, and ultrasonic. As a result, it is possible to detect and mitigate a disagreement between sources.

**3. Identify any standards, guidance, industry practices and sector specific requirements referenced in association with managing public or private sector cybersecurity risk to PNT services.**

There are several well-known practices used by industry to protect against jamming of space-based PNT signals. These include, but are not limited to:

- Radio frequency filtering in the antenna and in the GNSS receiver.

- Automatic detection of higher incident signals in the GNSS receiver by monitoring Automatic Gain Control (AGC).
- Multi-band, multi-constellation GNSS receivers.

Advanced anti-jamming concepts are also being explored by the automotive industry. For example, low-cost adaptive antenna arrays may be used to perform beamforming (i.e., steering the antenna gain pattern toward satellites and away from jammers). In addition, when GNSS signals are compromised, tightly coupled Kalman filter designs can dynamically assign higher weighting to IMU and perception sensors.

At the same time, federal law prohibits the operation, marketing, or sale of any type of jamming equipment that interferes with authorized radio communications, including Global Positioning Systems. Certainly, vigorous investigation of space-based PNT jamming reports and enforcement in the case of confirmed attacks is an important component in the effort to protect against would-be attackers.

With respect to spoofing, many proprietary anti-spoofing software features are being designed into automotive GNSS chipsets. These features can help detect and reject false signal broadcasts.

Published research and standards provide considerable information about attacks on PNT, mitigations for such attacks, and potential classes of attacks on both vehicles and related systems. These papers and standards, which may prove helpful to NIST, include:


- IETF Network Time Services for NTP (RFC Editor Queue) Security Considerations, https://tools.ietf.org/html/draft-ietf-ntp-using-nts-for-ntp-28
- GNSS spoofing and detection, ML Psiaki, TE Humphreys - Proceedings of the IEEE, 2016
- Wang, F.; Li, H.; Lu, M. GNSS Spoofing Detection and Mitigation Based on Maximum Likelihood Estimation. *Sensors* 2017, *17*, 1532.
- Nighswander, Tyler, et al. "GPS software attacks." Proceedings of the 2012 ACM conference on Computer and communications security. 2012.
- Shepard, Daniel P., et al. "Evaluation of smart grid and civilian UAV vulnerability to GPS spoofing attacks." Radionavigation Laboratory Conference Proceedings. 2012.
- Bittl, Sebastian, et al. "Emerging attacks on VANET security based on GPS Time Spoofing." 2015 IEEE Conference on Communications and Network Security (CNS). IEEE, 2015.


**4. Identify and describe any processes or procedures employed by the public or private sector to manage cybersecurity risks to PNT services.**

The use of multiple, independent, cross-validated sources of PNT information is one way in which threats to PNT services can be at least partially mitigated. In addition, the use of measurements of physical reality to constrain potential variations in valid PNT data has some potential for limiting potential errors.

In addition, the same cybersecurity risk management strategies used elsewhere may be applied to PNT. These strategies include:

- Running processes with the least privilege possible
- Performing code validation and verification

- Running PNT code on a trusted and validated computing platform that only executes validated, signed code
- Protecting GNSS signal sources, receivers, and software utilizing defense in depth strategies
- Actively maintaining security patches on all GNSS-related devices
- Utilizing well-studied and well-validated implementations of security-related code
- Subjecting GNSS signal sources and receivers to frequent red team attacks
- Ensuring that PNT hardware and software properly handle all possible inputs and edge cases

There is growing interest in using vehicle crowd sourcing to detect potential jamming and spoofing in real-time and report these incidents to cloud-based repositories. For example, if three or more vehicles report elevated AGC levels in the same location and report these incidents to a common server, the common server can apply artificial intelligence to identify a likely jammer or spoofer and local authorities can be notified. If a common definition of a jamming or spoofing indicator were developed, the implementation of this capability for vehicles with connectivity may be possible.

**5. Identify and describe any approaches or technologies employed by the public or private sector to detect disruption or manipulation of PNT services.**

There are several papers that identify and describe approaches or technologies employed to detect disruption or manipulation of PNT services that may be of interest to NIST. These include:

- Wang, F.; Li, H.; Lu, M. GNSS Spoofing Detection and Mitigation Based on Maximum Likelihood Estimation. *Sensors* 2017, *17*, 1532.
- Khanafseh, Samer, et al. "GPS spoofing detection using RAIM with INS coupling." 2014 IEEE/ION Position, Location and Navigation Symposium-PLANS 2014. IEEE, 2014.
- Jafarnia-Jahromi, Ali, et al. "Detection and mitigation of spoofing attacks on a vector-based tracking GPS receiver." *Proc. ION ITM* (2012): 790-800.
- Psiaki, Mark L., et al. "GPS spoofing detection via dual-receiver correlation of military signals." *IEEE Transactions on Aerospace and Electronic Systems* 49.4 (2013): 2250-2267.
- Cavaleri, Antonio, et al. "Detection of spoofed GPS signals at code and carrier tracking level." *2010 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*. IEEE, 2010.
- Montgomery, Paul Y. "Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer." *Radionavigation Laboratory Conference Proceedings*. 2011.
- Jafarnia-Jahromi, Ali, et al. "GPS vulnerability to spoofing threats and a review of antispoofing techniques." *International Journal of Navigation and Observation* 2012 (2012).

**6. Identify any processes or procedures employed in the public or private sector to manage the risk that disruption or manipulation to PNT services pose.**

Certainly, processes or procedures employed to manage the risk posed by disruption or manipulation of PNT services depend on the individual needs or requirements of the specific public or private sector organization. However, examples of the types of processes or procedures that could be used include:

- Employment of anti-spoofing or anti-jamming techniques and algorithms
- Employment of algorithms and systems that are tolerant of, or insensitive to, the loss or perturbation of GNSS data
- The use of alternate, backup, or secondary PNT data sources to validate, correct, or disable PNT sources
- Design and implementation of systems that function without the availability of PNT services
- Cryptographic solutions for military GPS
- The use of non-PNT data sources such as camera or LIDAR to confirm or invalidate PNT signals

There is always an opportunity to learn and benefit from additional research into managing the risk that disruption or manipulation to PNT services pose. The work that is currently underway at the U.S. Department of Transportation, as directed in the *National Timing Resilience and Security Act of 2018*, on a land-based, resilient, and reliable alternative timing system to serve as a complement to and backup for GPS is important research that can help advance the resilience of PNT services used in transportation applications.

The U.S Department of Transportation's recently announced funding opportunity for the establishment of a Highly Automated Transportation Systems Research University Transportation Center (UTC) is also promising. According to the funding opportunity, in recognition of the importance that resilient PNT services have on supporting automated systems, the UTC will be focused on supporting secure cyber resilient PNT receivers for use in automated systems and carry out research to support the development of standards and/or prototypes. This is potentially helpful research that can be leveraged by the automotive industry.

**7. Identify and describe any approaches, practices, and/or technologies used by the public or private sector to recover or respond to PNT services posed.**

In general, systems that are designed to be resilient to the loss or perturbation of GNSS data will be more capable of recovering from a PNT disruption than those that are not. For example, for automated and autonomous vehicle localization, space-based PNT are only one component of a much more complex system design. No automated or autonomous vehicle on the market today uses GNSS signals exclusively for real-time vehicle control. GNSS signals are commonly combined with IMU measurements, wheel odometry, a High Definition map, and perception sensors to localize the vehicle to a specific lane on the road. Therefore, if GNSS is jammed or spoofed, other sensor information is available to compare against GNSS data in real-time.

**8. Any other comments or suggestions related to the responsible use of PNT services.**

All automated and autonomous vehicles use redundant inertial and perception sensors to supplement GNSS. These typically include gyroscopes, accelerometers, cameras, LIDAR, ultrasonic sensors, radar, and a High Definition map. Nevertheless, GNSS is the preferred technology for time alignment to UTC and localization to a global reference datum such as WGS-84 and NAD-83. High Definition maps contain attributes that are expressed in a global reference datum, so GNSS is the primary mechanism to align the vehicle to the reference datum in the map. Similarly, whenever sensors need to be time-aligned to a common reference, GNSS is almost always the technology of choice.

GNSS is obviously vulnerable to circumstances that can compromise accuracy or degrade GNSS-dependent services. These include jamming and spoofing, but also more commonplace problems such as

ionospheric delay, multipath, poor satellite visibility in tunnels and parking garages, and the risk of errors in the GNSS satellite signals themselves. For these reasons, the automotive industry will almost certainly continue to take advantage of supplemental sensors to enable vehicle functions when GNSS is compromised. Going forward, ongoing engineering investment will continue to improve Automotive Safety Integrity Level (ASIL) integrity levels within automotive GNSS equipment.

Strong standards and practices for validation, authentication, and verification of PNT signals and services should continue to be embraced by industry. To prevent spoofing attacks, authentication should be considered for the civilian GPS signal. Moreover, authenticated ground-based PNT should be available as a supplement and as a backup to satellite-based GPS.

Once again, Auto Innovators appreciates the opportunity to comment on this RFI. We welcome the opportunity to answer any further questions or provide any additional information on the importance of resilient PNT services to the automotive industry.

Sincerely,

Hilary M. Cain
Vice President
Technology, Innovation & Mobility Policy