RNT Foundation
4558 Shetland Green Rd
Alexandria, VA 22312

29 November 2018

Docket No. DOT-OST-2018-0149

Comments on: *Preparing for the Future of Transportation: Automated Vehicles 3.0 (AV 3.0).*

The Resilient Navigation and Timing Foundation comments that the Department of Transportation's Automated Vehicles 3.0 (AV 3.0) fails to sufficiently address the vulnerabilities of the Global Positioning System (GPS) and America's lack of a resilient positioning, navigation, and timing (PNT) architecture.

Successful deployment of automated vehicles of all kinds - maritime, aviation, land, and rail – and their integration into our national transportation system will depend upon having ubiquitous, wireless, highly dependable and resilient PNT services. Yet America's current PNT architecture is highly reliant, and in many cases exclusively relies, upon space-based GPS signals.

Unlike terrestrial systems, signals from space are weak and easy to disrupt. And GPS signals are weaker than most space-based signals. Also, the well-known characteristics of GPS signals make them easy to spoof. Studies have shown that instances of GPS signal disruption are occurring with greater frequency and that the devices used to intentionally interfere with these signals are increasing in sophistication.[i]

Rather than highlighting this as a significant issue upon which rests the success or failure of automated vehicles, AV 3.0 barely addresses it.

- Service denial (jamming or inadvertent interference from a natural or man-made source) is not mentioned at all, and,

- While GPS spoofing is mentioned once, efforts to address the problem are misrepresented. Table 2, page 60, lists two "standardization-related activities" that supposedly address this problem. Yet neither of the listed standards address navigation or timing systems.

GPS signal vulnerabilities pose several challenges for automated vehicles and the systems upon which they depend:

Initializing Navigation Systems – On-going navigation of automated vehicles will rely largely on hyper-accurate maps, cameras, wheel counters, Lidar and other on-board sensors that do not require external input. However, external reference positioning will still be required to initialize systems after complete shutdowns. If such a vehicle is in an underground garage, an urban canyon, or if GPS is disrupted in the area, initialization of vehicle navigation could fail.

Connected Cars/Intelligent Transportation Systems - **Network Integrity** – Connecting vehicles with each other and coordination/control systems via wireless networks is essential for intelligent transportation systems. GPS timing signals are essential for synchronization and proper functioning of wireless networks.[ii] Disruptions of GPS signals can disable or degrade these networks.

Connected Cars/Intelligent Transportation Systems – Own Location – Connected cars will communicate their location to other cars and ITS components. Most approaches call for communicated vehicle locations to be derived from GPS. The ease with which GPS signals can be denied or imitated makes this risky.

The Secretary of Transportation can address the challenges posed by GPS vulnerabilities and ensure our nation's transportation system always has the PNT services it needs by fulfilling the department's long-standing obligation to acquire a national backup capability for GPS.

National Presidential Security Directive 39 directs the Secretary to, in consultation with the Secretary of Homeland Security, acquire such a capability to protect our national and economic security when GPS signals are not available. Despite this mandate having stood for fourteen years, the department has failed to do so.

The government committed to establishing an eLoran system for this purpose in 2008, and again in 2015. These commitments were based upon rigorous studies and analyses by interagency teams supported by academic centers of excellence.

eLoran signals can provide wireless, very difficult to disrupt positioning, navigation, and timing information via completely different phenomenology than GPS. They are precise enough to meet projected 5G and many other network and GPS backup needs. While GPS signals are weak, very high frequency signals from space, eLoran signals are very powerful, low frequency signals from transmitters on Earth. Something that could impact one type of signal would be very, very unlikely to impact the other. Users who access both would be virtually immune to disruption.

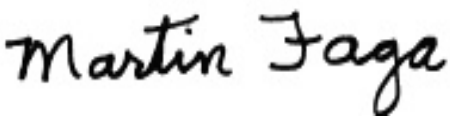
We support the government's policy for acquiring a backup capability for GPS to protect our national security and economy against GPS disruptions and failures. We endorse the government's multiple decisions to implement eLoran technology. We urge prompt action.

To expedite implementation and minimize the burden on government of establishing this capability, it should be accomplished via a service-level contract with a commercial provider. With the government's commitment to subscribe to eLoran signals, a commercial entity can easily and quickly put signals on air. If the commercial entity is allowed to also provide value-added, fee-based services, the government could share in the revenue and recoup its own subscription costs.

Our national adversaries have on-going programs of GPS disruption over broad areas. Local micro disruptions by individuals with "personal" jammers are growing in frequency and sophistication. Both types of challenges show our national vulnerability and reinforce the need for prompt action.

Acting on this issue will establish an environment within which autonomous vehicles, aircraft and vessels are able to safely and efficiently navigate.

Dana A. Goward
President



Martin C. Faga
Chairman of the Board

The Resilient Navigation and Timing Foundation is a scientific and educational charity 501(c)3 incorporated in Virginia - 888-354-9109, Inquiries@RNTFnd.org

[i] STRIKE3 Presentation to US National PNT Advisory Board 16 May 2018
[ii] Alliance for Telecommunications Industry Solutions Technical Report "GPS Vulnerability" ATIS-0900005 September 7, 2017