Docket #DOT-OST-2018-0210 January 25, 2019

Office of the Secretary (OST)
U.S. Department of Transportation (DOT)
1200 New Jersey Avenue S.E.
Washington, DC 20590

In RE: *Notice of Request for Comments: V2X Communications.* Comments of Rajant Corporation.

Thank you for the opportunity to provide comments on V2X for automated vehicles. Rajant Corporation supports the efforts of US DOT to develop a robust regulatory framework to ensure security and efficiency in the emerging automated transportation field.

About Rajant Corporation:

Rajant Corporation develops, manufactures and deploys highly secure wireless communications technology. Rajant was the first to build for the U. S. Military its patented Kinetic Mesh® technologies using Rajant's BreadCrumb® wireless LAN technology. These network components are designed for remote and rugged terrains and harsh physical environments like those seen by troops deployed throughout the world. Our technologies are battle-proven to support the mission-critical communications to simultaneously overcome the challenges of environmental adversity, diverse infrastructure and security. Rajant's key differentiation point, its ability to maintain connectivity while assets are mobile and in motion, is the cornerstone of Rajant's success. Rajant has a proven track record of performance in a number of high-profile military programs, such as C-RAM, RAM-Warn and others. Our military products have achieved NSA certification which mandate the highest level of security prior to being fielded within the Department of Defense (DOD). Rajant networks ensure secure transmission and reception of highly sensitive data, voice and video in combat conditions – conditions where a breach in security can result in fatal consequences.

General Comments

With extensive experience in wireless communication and cybersecurity, Rajant supports a regulatory framework that encourages innovation, adoption and security. With respect to V2X AV communication, Rajant offers the following general comments:

- Rajant supports the technology-neutral stance of US DOT. Both DSRC and C-V2X possess unique advantages. A technology-neutral stance will allow both platforms to attract investment and innovation.
- Rajant supports the reservation and dedication of the 5.9 GHz spectrum for automated transportation.
- Interoperability between DSRC and C-V2X is feasible and preferable and does not pose a significant technical burden.
- Rajant agrees with mandating FIPS-140 Level 3 HSM as discussed in NHTSA 2016-0126.

200 Chesterfield Parkway ● Malvern, PA 19355 ● tel (484) 595-0233 ● fax (484) 595-0244
www.rajant.com

Question #2:

Rajant Corporation recommends US DOT continue to reserve the 5.9 GHz spectrum exclusively for automated transportation and avoid unanticipated system conflicts.

Question #3:

Interoperability between DSCR and C-V2X is technically feasible and a preferable policy for US DOT. Communications can switch between ports as long as there are available channels. Further, additional paths of communication allow for a more robust technological environment.

Question #7:

Rajant supports mandating use of the FIPS-140 Level 3 Hardware Security Module design as a minimum standard. As stated in the V2V NPRM (NHTSA 2016-0126), hardware and software vulnerabilities are acute at the communication interfaces and thus, "Security of the interfaces must be the highest priority when developing the system." (*Federal Register,* vol. 28, no. 8, January 12, 2017, p. 3918). Rajant concurs and fully supports this statement and believes that any V2X system must be designed with robust, effective cybersecurity protections at its initial conception.

Delaying implementation of cybersecurity procedures and layering in or patching at a later date not only will be an expensive proposition, it also has the potential to threaten public safety and public acceptance of automated transportation. Hard-won experience has shown that *post facto* technological fixes are usually in response to a significant incident. Negative incidents in the early adoption of automated transportation have the potential to delay adoption and realizing the benefits of automation.

In NHTSA 2016-0126, the Agency mooted three options for the implementation of V2V cybersecurity including a direct mandate, performance-based physical security and no physical security alternative. Due to the critical necessity of robust cybersecurity and the safety mandate for NHTSA, voluntary standards (the "No Physical Security Alternative" mooted in NHTSA 2016-0126) are not appropriate public policy.

Rajant Corporation previously commented on the importance of mandated cybersecurity in DOT-OST-2018-0149. We would like to submit those comments as part of the record with respect to V2X:

> As US DOT notes in *Automated Vehicles 3.0,* situations exist where significant benefits to the public are not realized due to weak or absent market incentives (P. 12). In such situations US DOT acknowledges a responsibility to engage in proactive policy. Further, US DOT recognizes this problem in research activities, stating "Public investments in research are often warranted to support the development of potentially beneficial technologies that are not easily commercialized because the returns are either uncertain, distant, or difficult to capture." (P. 13) US DOT proceeds to specifically cite cybersecurity as residing within that arena of public investment.

Gains from robust cybersecurity and reducing cyber risk mirror those from research activities in that they are difficult to quantify, lack certainty and such gains are challenging for individual firms to monetize or show return on investment. In addition, the benefits from increased safety accrue not only to owners/operators of vehicles, but also to pedestrians, public infrastructure and private property. Such gains are difficult to capture and realize, resulting in underinvestment, thus justifying a public policy response.

But market incentives are not only challenged in responding to safety concerns, market incentives might turn perverse and result in *reduced* cybersecurity and *increased* risks. Given the many players in the AV industry and its highly competitive nature, the incentive exists for a given company (or companies) to move forward without robust cybersecurity protections in order to come to market with a product. A given company may decide to "chance it" in the market when the alternative is to fall behind its competitors. Furthermore, as AASHTO states in its comment, the AV industry is a "very competitive environment" which is "challenged to reach consensus." **In a voluntary regulatory regime with weak, absent or perverse market incentives, operating in the context of very high competition, just one bad actor (company) could set the entire industry back by rushing to introduce an unsafe product.**

The competitive market system is highly efficient and effective in advancing technology and innovative design. However, the competitive market is not well-suited to advancing safety and addressing cybersecurity and cyber risk. The difficulty in capturing gains from safety and the resulting underinvestment in safety was a causal factor in the creation of NHTSA in 1970.

Thank you for the opportunity to comment. Rajant Corporation and its technical and management staff are available to assist and advise US DOT on these vital issues.

Submitted Respectfully,

/s/ Robert J. Schena /s/
Chief Executive Officer
Rajant Corporation

200 Chesterfield Parkway ● Malvern, PA 19355 ● tel (484) 595-0233 ● fax (484) 595-0244
www.rajant.com