Memorandum to the State of Oregon Task Force on Autonomous Vehicles

To: Subcommittee on Cybersecurity and Long-Term Policy
From: Tyfone, Inc.
Date: July 27, 2018
Re: Legislation language regarding Cybersecurity

Dear members of the subcommittee,

Thank you for the important work you are doing regarding cyber threats that autonomous vehicles on Oregon roads will face in the future. We are concerned about it as well and we would like to respectfully make recommendations for you to consider for the legislation regarding cybersecurity.

We will first provide background of our expertise, followed by the problem statement and conclude with recommendations for you to consider.

Background
Tyfone is an Oregon based cybersecurity company that has customers including the US Department of Defense, Electric Power Research Institute (EPRI), Jaguar Land Rover, and two of the Top 10 Credit Unions in the United States. Tyfone’s equity holders include Jaguar Land Rover, In-Q-Tel, and General (Retd) David Petraeus.

The company has over 130 patents related to cybersecurity and our approach to cybersecurity is beginning to be well-recognized in the marketplace, especially for applications in critical infrastructure. An example critical infrastructure application of our technology in partnership with EPRI to protect US electric power infrastructure, can be seen on YouTube here: https://www.youtube.com/watch?v=hbWO5Qzsbho.

Problem Statement
The purpose of this memo is to highlight two problems facing the subcommittee as it relates industry standards.

(1) Current industry standards vary dramatically and a large majority of them do not have sufficient protections for critical infrastructure applications such as connected and autonomous vehicles.

(2) At any given point in time not all industry standards are created equal. Given connected and autonomous vehicles will go across multiple industries from cloud companies to car manufactures industry standards are different and are interpreted differently.

Recommendations

Adopt California legislation on cybersecurity with the following two changes:

(1) Change "...meet appropriate and applicable current industry standards..." To "...meet appropriate and applicable critical infrastructure industry standards..."

(2) Add a final sentence that clarifies what cybersecurity nee "Appropriate and applicable industry standards means standards that maximize data security, privacy and safety of lives."

Thank you!