



8 July, 2018

Ms Rahila David
Project Manager
National Transport Commission
Level 3/600 Bourke Street
MELBOURNE VIC 3000

Dear Ms David,

**Submission re: Safety Assurance for Automated Driving Systems (ADS)
Consultation Regulation Impact Statement**

The Internet of Things Alliance Australia (IoTAA) is pleased to have the opportunity to make a submission regarding the Safety Assurance for Automated Driving Systems Consultation Regulation Impact Statement.

A significant factor in assuring safety, and therefore trust, for Automated Driving Systems is assessing and managing safety threats due to the significant underlying internet (of things) infrastructure that supports Automated Driving Systems. This applies across all elements of ADS from vehicle management (e.g. updates), vehicle to vehicle communications (e.g. collision control) and roadside to vehicle communications (e.g. traffic warnings).

Key points to be noted:

- While the increased use of internet (of things) technology greatly increases capability and use, it also increases susceptibility to third party attacks
- Internet of things and internet cyber security laws and regulations are immature and where they exist are largely voluntary
- privacy and sharing rules regarding vehicle and personal data may be required to limit access and protect citizens

To address the points above, for all IoT contexts, IoTAA has developed an IoT security strategy <http://www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA-Strategic-Plan-to-Strengthen-IoT-Security-in-Australia-v4.pdf> which outlines minimum recommended industry and government action to mitigate and protect users from poorly protected internet of things devices and services. This includes the development of an IoT Trust Mark Scheme to:

- encourage IoT device manufacturers to develop secure IoT devices and services;
- enable users of IoT devices to have confidence in the security and privacy features claimed in an IoT device; and

- provide IoT testers with a framework for predictable, standardised and repeatable testing of devices.

The *Trust Mark Scheme* cover the testing of IoT devices to ensure the security and privacy of:

- data generated by IoT devices;
- data carried to and from IoT devices;
- data stored in IoT devices;
- consumers using IoT devices; and
- actuators driven by IoT systems.

The *Trust Mark Scheme* deals with IoT devices associated with, but not limited to:

- home use by consumers;
- business use in the office environment;
- industry use in operational systems;
- government;
- critical infrastructure; and
- organisations of significant national interest.

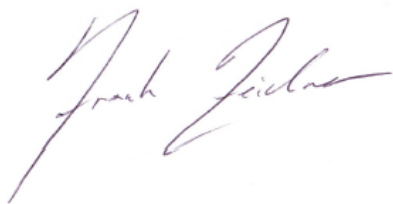
The IoTAA *Trust Mark Scheme* provides specific interpretation of standard security and privacy controls in the IoT context and encourages security in the design and development process. A key requirement is the:

- testing of the claims related to secure use and storage of information obtained
- testing of the claims related to integrity of the operating system and application

Given the safety implications for ADS, IoTAA would recommend consideration by given to applying an “ADS cybersecurity and data trust mark” along the lines described above.

We welcome the opportunity to discuss our thoughts in more detail.

Yours sincerely,



Frank Zeichner

Chief Executive Officer
IoT Alliance Australia
Frank.zeichner@iot.org.au
www.iot.org.au

Matt Tett, Chair, IoTAA Cybersecurity and Network Resilience work stream

www.iot.org.au