RazorSecure Limited – Written evidence (AUV0018)

Letter from Alexander Cowan, CEO, RazorSecure Limited

1. We wish to respond to your “Call for Evidence” on Autonomous Vehicles. RazorSecure Limited is a business based around cyber security of mobiles assets with a particular focus on the implications in the transport industry.

2. We are currently developing solutions in the aviation and rail industry, and we consider autonomous vehicles to be a significant future area for development in both cyber security and passenger safety. As such we would be happy to provide additional evidence as a specialist in cyber security for the transport industry.

3. I wish to respond to the following questions in respect to the call for evidence.

2. What are the potential user benefits and disadvantages from the deployment of autonomous vehicles?

4. As a son and step father, one of the key areas that I see autonomous vehicles being used are in increasing mobility of our population. Currently this area is being serviced by the taxi and private hire industry, however during peak times it is very difficult to get access to a driver, outside of big cities, without a pre-booking days in advance.

5. It is not just the passengers of autonomous vehicles that will see benefits from their adoption, but also the care givers, guardians and relatives of users without access to a traditional vehicle.

6. As the son of a pair of elderly parents, I see mobility as one of the true keys to their continuing independence. From visiting supermarkets to hospital appointments, having access to an autonomous vehicle would allow me to ensure they are able to maintain independence without disrupting my usual work hours and productivity.

7. As a step father to a young adult, I am often called upon to ensure my son is delivered to college, sports training and activities with friends. Having access to an autonomous vehicle would allow me to ensure he is delivered safely to the correct destination without the traditional disruption. Even though he has recently completed his driving test, given the current costs of car insurance it is prohibitively expensive to get him access to his own vehicle.

4. How much is known about public attitudes to autonomous vehicles?
8. Security will be a key consideration in public attitudes towards autonomous vehicles. The Department for Transport has published papers on cyber-security in the rail industry (ref: “Rail Cyber Security – Guidance for Industry”), and particularly around the multi-layered security approach required to ensure these vehicles are safe for public use.

9. With increasing adoption of autonomous vehicles, any incidents will be reported in the media and likely face extreme scrutiny. A significant cyber-attack could see the entire network of autonomous vehicles being taken offline. Therefore, it is key that the layered approach to security including firewalls, intrusion detection, encryption and software/hardware assurance is considered before mass adoption can occur.

10. This media scrutiny has already been occurring in California where incidents with the Google self-driving vehicles are analysed by the media who are flagging for any potential safety issue with the technology. Failure to address security and safety concerns, will erode public trust in the technology and undermine future adoption.

8. How effective are Innovate UK and the CCAV in this area?

11. The CCAV scheme is a very positive step towards providing funding for projects within the UK. The commercial focus is admirable; however it is challenging for SMEs to access. RazorSecure spent considerable time investigating the CCAV2 scheme, but were unable to put together a consortium within the time frame to place a project bid.

12. The consortium requirement certainly places a lot of extra pressure in what is an already challenging area. While we can see the benefits in terms of greater engagement and higher chance of success, it was a deciding factor in us not continuing to invest time with that programme.

12. Does the Government have an effective approach on data and cybersecurity in this sector?

13. It is important to recognise that future autonomous vehicles will be significantly different from the current private hire vehicles that are in use today. The environment that will exist will be more akin to a new form of mass public transportation and will rely heavily on the hardware and software manufacturers over the operators to ensure the safety and security.

14. Cyber security will be critically important and thus hardware and software manufacturers must be required to deliver updates to vehicles over their entire lifetime. This is a growing issue in the security industry, as devices are often only certified as secure when they are manufactured for the first time. This means that new security
vulnerabilities may not be considered in the ongoing production of devices, and in the future vehicles.

15. In addition, it is important that hardware/software manufacturers and operators are required to put in place a multi-layered approach featuring techniques such as firewall, encryption, intrusion detection and active response even when not connected. Early warning of attacks and breaches is key to ensure that they can be managed quickly and safely without compromising the availability of the technology.

16. The RazorSecure team has experience with cyber security in rail, aviation, space and defence. We would welcome the opportunity to help define the processes and standards and to create an environment for the UK to become a world-leader in safe and secure autonomous vehicles.

13. Are further revisions needed to insurance, regulation and legislation in the UK to create an enabling environment for autonomous vehicles?

17. For an effective, safe and secure mass deployment of autonomous vehicles, it is important that the correct regulation is put in place regarding cyber security.

18. These rules are currently being developed for other areas of critical national infrastructure, and it is important to recognise that a connected network of autonomous vehicles would represent a new form of mass public transportation.

19. In addition to the usual certification and assurances that are required to deliver a product to market, it is critical that manufacturers are required to support the product with security updates over the vehicle’s lifetime.

20. In a recent security incident, a Tesla Motors vehicle was able to be hacked remotely and the hackers could activate the vehicle’s brakes while it was in motion (ref: “Team of hackers take remote control of Tesla Model S from 12 miles away” – The Guardian September 20th 2016). The vehicles were updated via an over-the-air update within days to close the exploit, but this relied on the hackers announcing the breach and also the manufacturer to provide a quick response.

21. It is therefore vital that manufacturers are required to implement a multi-layered approach focusing on security and early detection of breaches.

15. What does the proposed Modern Transport Bill need to deliver?
22. In the area of delivering “safe technology in the autonomous vehicles industry” (ref: The Queen’s Speech 2016 – 18th May 2016), we would look for the Modern Transport Bill to deliver:

- A requirement cyber-security to be a key consideration in the health and safety of passengers
- A requirement for hardware and software manufacturers to deliver security updates for the lifetime of the vehicle
- A requirement for a multi-layered approach to cyber security in autonomous vehicles

24 October 2016