Submitted by the UK to the informal meeting of ITS-AD on 20th September 2016

Cybersecurity and Data Protection

The UK is grateful to Germany and Japan in developing the guidelines for measures ensuring cybersecurity and data protection of connected and automated vehicles and the ambition of moving towards globally harmonised requirements on cybersecurity. The UK is pleased to support the proposal.

We agree that international coordination and collaboration is required, which is why the UK supports the draft declaration on "Development and widespread utilization of advanced technology for vehicles and roads" submitted ahead of the forthcoming G7 transport ministers meeting.

We would also be keen to stress the importance of a broadly based approach to security that encompasses personnel, physical and cyber security and the interactions between them. Security is vital for the safety, resilience and integrity of the transport network, in addition to the important aspect of data protection. The connected and autonomous vehicle system (including any web, highways or other services that support it) must be secure by design. A failure to take appropriate measures could lead to loss of public trust in the technology.

These are unique challenges for the automotive sector that require a unique approach. The objectives of regulators and industry coincide on these matters, which provides tremendous grounds for collaboration.

We consider that guidelines are the most appropriate measure at this stage, in light of the pace of development in this area. To avoid constraining innovation, where appropriate, these guidelines should be outcome rather than output-based. At the same time, where industry supports the early identification of technical solutions we should not rule this out. In this way we can work towards a shared understanding of what constitutes good practice and identify how this can be achieved in the marketplace.

We believe it is vital that we work at pace on these commitments. The proposals submitted to this working group from Germany and Japan are a positive first step. Nonetheless, the UK is keen to drive this agenda forward.

The UK government's Centre for Connected and Autonomous Vehicles is coordinating activity in automotive cybersecurity, in collaboration with the relevant government security agencies who are specialists in protective security (physical, personnel and cyber) and information assurance. We have developed a draft set of high level principles for the security of the connected and autonomous vehicle system, ranging from board-level engagement, to supply chain management, to what we could expect of the ITS infrastructure that vehicles interact with.

We will shortly be approaching vehicle manufacturers, as well as Tier-1 and Tier-2 suppliers with a survey. The purpose of this is to provide a better understanding of industry's opinion on the issues, the principles we have developed and possible ways forward. We would greatly value their engagement.

At the plenary meeting of WP.29 in November, we will be presenting further thoughts on how to achieve the vision of a secure connected and autonomous vehicle system, and to move towards globally harmonised requirements. We will share the interim findings from our industry survey once completed later this year or early 2017 along with the draft principles.