Department for Transport

Cyber security for automotive

Department for Transport

Challenges for the automotive industry

- **Cultural:**
  - Cyber security is new to the industry
  - They need to get the right structures and organisation in place to make cyber security business as usual
- **Technical:**
  - The long development time and life cycle of vehicles adds complexity
  - How to manage risks in the supply chain and interactions with third parties (such as after market telematics devices)
- **Governmental:**
  - There is no regulatory framework for what manufacturers should do
  - Standard bodies (ISO, ITU, SAE) are producing initial guidance in this area

Department for Transport

Our approach to cyber security

- Our **vision** is that “The UK’s transport sector remains **safe**, **secure** and **resilient** in the face of cyber threats, and able to **thrive** in an increasingly interconnected, digital world”
- **We want to ensure an appropriate level of protection** for vehicles, and the road side infrastructure they talk to, from unauthorised access, control or interference
- Our aims in support of this are to:
  - **Understand** the cyber threat and the vulnerabilities for the transport sector
  - **Mitigate** cyber risks and take appropriate action to protect key assets
  - **Respond** to cyber incidents effectively and ensure that lessons are learnt
  - **Promote** cultural change, raise awareness and build cyber capability

Department for Transport

What are we doing?

- *Promote* - NCSC/CPNI hosted **automotive information exchange** (Feb 2017)
- *Promote* **- Cyber security principles** for CAV (April 2017)
- *Mitigate* - Collaborating on cyber security for **connected corridors** with EU partners
- *Mitigate* - Chairing a **task force on cyber security** within the UNECE World Forum for the Harmonization of Vehicle Regulations (draft paper 2018)
- *Respond* - **Incident response** and reporting mechanisms with NCSC (2017)

Department for Transport

UNECE

UNECE task force on cyber security and software updates

- The group includes trade bodies, industry and government
- The aims of the group are to:
  - Define requirements for addressing cyber threats
  - Define requirements for software update management with respect to safety type approval
  - Define guidance or measures for how to achieve this
- Aim to deliver these in 2018 to Working Party 29
  - The output may then be adopted as a regulation or resolution
- We recognize the need for agreeing something quickly
  - Standards may be instrumental but we must be agile as this is a rapidly developing area