News story: New generation of smart cars will now be better protected from hackers

A new generation of internet-connected cars will have to be better protected from hackers, under tough new government guidance issued today (6 August 2017).

Smart vehicles are increasingly becoming the norm on British roads – allowing drivers to access maps, travel information and new digital radio services from the driving seat.

But while smart cars and vans offer new services for drivers, it is feared would-be hackers could target them to access personal data, steal cars that use keyless entry, or even take control of technology for malicious reasons.

Now new government guidance will ensure engineers developing smart vehicles will have to toughen up cyber protections and help design out hacking. The government is also looking at a broader programme of work announced in this year's Queen's speech under the landmark Autonomous and Electric Vehicles Bill that aims to create a new framework for self-driving vehicle insurance.

The legislation will put Britain at the centre of the new technological developments in smart and autonomous vehicles – but while ensuring safety and consumer protection remain at the heart of the emerging industry.

Measures to be put before Parliament mean that insuring modern vehicles will provide protection for consumers if technologies fail.

This comes alongside new guidance that means manufacturers will need to design out cyber security threats as part of their development work.

This will cement the UK as a world-leading location for research and development for the next generation of vehicles. And it forms part of the government's drive to ensure the country harnesses the economic and job-creating potential of new tech industries.

Transport Minister Lord Callanan said:

> Our cars are becoming smarter and self-driving technology will revolutionise the way in which we travel. Risks of people hacking into the technology might be low, but we must make sure the public is protected. Whether we're turning vehicles into wifi connected hotspots or equipping them with millions of lines of code to become fully automated, it is important that they are protected against cyber-attacks.
>
> That's why it's essential all parties involved in the manufacturing

> and supply chain are provided with a consistent set of guidelines that support this global industry. Our key principles give advice on what organisations should do, from the board level down, as well as technical design and development considerations.

Mike Hawes, Society of Motor Manufacturers and Traders Chief Executive, said:

> We’re pleased that government is taking action now to ensure a seamless transition to fully connected and autonomous cars in the future and, given this shift will take place globally, that it is championing cyber security and shared best practice at an international level. These vehicles will transform our roads and society, dramatically reducing accidents and saving thousands of lives. A consistent set of guidelines is an important step towards ensuring the UK can be among the first – and safest – of international markets to grasp the benefits of this exciting new technology.

The government will continue to support and work collaboratively with industry to make sure vehicles are protected from cyber-attacks. The guidance principles published today will form a key part of these discussions .