DAC BEACHCROFT

CALL FOR EVIDENCE: DEVELOPING THE AUTOMATED VEHICLES REGULATORY FRAMEWORK

THE RESPONSE OF DAC BEACHCROFT LLP

ABOUT US

DAC Beachcroft LLP is a leading international legal business with offices across the UK, Europe, Asia Pacific and the American continents.

We partner with our clients to help them achieve sustainable growth and to defend their business and reputation. We do this by taking a tailored approach to providing commercial, transactional, claims, risk and advisory legal services.

We are recognised leaders in Insurance, Health and Real Estate and draw on the knowledge, industry experience and commercial expertise of our outstanding 2,200 lawyers and support colleagues in these sectors and beyond.

We are a forward-thinking business. We are committed to helping facilitate practical and beneficial legal reforms and technological innovation.

We have co-ordinated an automated vehicle (AV) team that draws from our strength as one of the UK's leading insurance law firms. Our AV team consists of 15 members from a wide range of specialist areas, including: motor claims and liability (civil and criminal), product liability and recall, data and cyber risk, technology, insurance regulatory, commercial, property and infrastructure and transport and logistics. As a global law firm we have access to legal experts in the US and across Europe, including our co-operation with BLD in Germany.

Our team has responded to every government, parliamentary and Law Commission consultation and call for evidence related to AVs and the future of motor going back to 2016. We have hosted training sessions and multijurisdictional seminars, spoken at industry-wide events, published articles and been featured in many interview panels. Our expertise in this area has been relied upon by insurers, trade organisations and trade publications.

GENERAL OBSERVATIONS

The benefits of 'safety-first'

The guiding principle of the development of ADS and the deployment of AVs needs to be ‘safety first’.

The government and parliament have adhered to this principle during the development of AV law to their credit, and this is one of the reasons why the UK is considered an international leader in this field.

The drafting of regulations that will allow for the full implementation of the AVA is the next crucial stage in the development of AV law, and the safety first principle must be adhered to as the regulations resulting from this call for evidence are drafted.

Many of the regulations that will come from this call for evidence will result in costs, sometimes significant ones, and CCAV is right to want to understand the costs and benefits of these. Safety, however, cannot be compromised in an attempt to lower costs at the outset; the opposite approach should be adopted at this early stage. The regulations and rules that come out of this call for evidence must be drafted with the focus entirely on safety and little to no regard for the costs of that safety. These extra costs will maximise safety gain, which will in turn build public trust and lower costs in the longer term.

Post initial deployment of AVs, with real world experience, the areas where regulations have demonstrated an overabundance of caution will become evident. The government can then relax those requirements, reducing costs only when it is safe to do so. The alternative is having to strengthen regulations after unwanted incidents, which would increase costs for compensators and damage public trust in ADS at a time when building trust is critical.

It is vital that adoption of ADS and related statutory reforms is done in a way to maximise public acceptance of these technologies. As the public is exposed to more AVs its trust in the technology will grow. This trust will be further strengthened by continued improvements in ADS.

If the government fails to inspire public confidence in ADS, take up will be limited. This, in turn will adversely impact the safety benefits that will be derived in the longer term from these new technologies. Conversely, a failure to adhere to the ‘safety first’ approach could lead to incidents involving ADS that would cause the media and public to turn against the technology, setting back mass market engagement by many years. It would also likely result in more incidents, increasing costs for compensators, emergency services and the NHS.

Regulatory development

We have had advanced sight of the ABI's response to the call for evidence, and we support the overarching themes, key principles, and detailed recommendations set out in the ABI’s submission, including but not limited to:

- The need for clear, consistent, and government-issued guidance that explains regulatory expectations, delineates responsibilities across actors in AV ecosystem and enables early and meaningful engagement between applicants, regulators, and insurers.
- The importance of aligning insurance requirements with vehicle approval and authorisation processes, ensuring that AVs are insurable at each phase of deployment and that consumers are protected through prompt, transparent and effective claims handling.
- The critical role of mandated, standardised data sharing between manufacturers, authorised entities, NUICOs, regulators and insurers to support liability determination, claims resolution, regulatory oversight, and post-incident learning, while upholding strong privacy and data protection safeguards.
- The value of clear distinctions between development, trial, transition and full deployment phases, with proportionate but robust insurance, data access and risk-management expectations at each stage.
- The necessity for evidence-based, interoperable regulatory frameworks, supported by harmonised standards and national coordination to reduce fragmentation, improve consistency and support continual improvement across regions and use-cases.
- The importance of integrating insurance and liability considerations into vehicle type approval and authorisation, including the availability of minimum post-incident datasets necessary for determining causation and applicable legal frameworks.
- The inclusion of strong enforcement, compliance, and assurance mechanisms, supported by adequately resourced regulators, to ensure confidence, fairness and accountability across the AV lifecycle.
- The need for transparency, accessibility, and safeguarding provisions, including protection for vulnerable and disabled road users, clear consumer communication and equitable access to redress.

Questions 1 – 6

No response given.

Question 7: In your view, what types of evidence should form the basis of an authorisation application?

Authorisation should be supported by evidence demonstrating that the vehicle, including ADS can operate safely and legally within the proposed operational design domain. This may include results from controlled testing, real world trials, cybersecurity assessments, incident logs, safety case documentation and third party evaluations. Evidence of compliance with international standards and any UK specific requirements should also be included. Independent verification can help ensure transparency and regulatory confidence.

Question 8: In your view, what evidence gathered at the vehicle type approval stage, if any, should be used to support an authorisation decision?

ADS should undergo rigorous testing to ensure that they are as safe as possible before they are authorised to be used on roads or other public places. This should apply both pre- and post-deployment, and when the ADS comes equipped on the vehicle and when it is an aftermarket product.

An approval regime based on both self-certification and third-party testing should be able to evolve to ensure the safety of new ADS as far as reasonably possible. The two can and should work together harmoniously and should improve consumer confidence and safety.

Safety needs to be assessed in a dynamic and continuing way to address recurring software changes and updates to an AV, vehicle recalls and modifications and changes in the relevant road and driving rules applicable in the post-authorisation period. Authorisation needs to be an ongoing process pre- and post-deployment.

The key evidence categories at the authorisation stage should include:

- Performance data across multiple environments (urban, rural, varied weather and lighting). This would include results from controlled testing in simulated and real-world environments, demonstrating performance, safety, and reliability under varied conditions
- Evidence of user behaviour, including compliance with AV instructions and the ability to manage updates
- The impact of the vehicle type on non-AV road users, particularly protected groups and vulnerable stakeholders
- Data relating to passenger experience
- Evidence that AVs, particularly those operated by NUICOs, are accessible to vulnerable customers
- Evidence relating to data protection compliance, as well as cybersecurity and resilience
- The ability to recognise and enforce safe operating parameters. This would include evidence of regulatory breaches and criminal conduct relevant to public safety

Question 9: In your view, do you think geofencing or environmental mapping have a role in operational design domain (ODD) approval, and why?

At their initial deployment, AVs will face many substantial challenges, including gaining the public's trust, safely integrating into the human-driven fleet and navigating a road network that does not yet have a fully modernised infrastructure (eg – nationwide 5G coverage) and was not designed for use by ADS.

It's important that AVs are not used in places where they cannot safely drive themselves, either because of the limitations of the road network (such as narrow country lanes and busy urban streets) or because the necessary infrastructure improvements have not yet been made. The

best way to prevent operators from attempting to engage self-drive in an inappropriate environment is by enforcing geofencing or environmental mapping.

As the road network or AV technology improves, it will be beneficial to re-evaluate whether the environmental map should be amended and, hopefully, expanded to increase the percentage of road network where it is safe to deploy ADS.

Until then, it is important that AVs be limited to where they can be safely used to reduce the likelihood of accidents and build public confidence in the technology.

Question 10

No response given.

Question 11: In your view, what should be considered when assessing whether an ASDE is of good repute?

Assessment of 'good repute' may appropriately draw on absence of relevant criminal convictions, history of regulatory compliance, and integrity of senior management. Consideration may also be given to ethical conduct in safety critical operations and the entity's record of transparency with regulators. The aim is to ensure that the an ASDE can be trusted to discharge ongoing safety obligations responsibly.

We have considered the operator licencing regime, where good repute is evaluated through a myriad of factors, most notably:

- Consideration of convictions
- Regulatory compliance
- Conduct and behaviour
- Financial stability
- Cooperation with enforcement agencies
- Rehabilitation

With regards to operator licencing, an individual or entity will be subjected to a mandatory loss of good repute if there are multiple serious convictions or offences relating to road safety.

Question 12: In your view, what should be considered when assessing whether an ASDE is of good financial standing?

It is of utmost importance that ASDEs be of good financial standing to ensure the continuing safe operation of AVs within their responsibility. Any failure by an ASDE to maintain ADS will risk the ADS-equipped vehicle becoming a liability, so the requirement to be of good financial standing must be a long term one.

Financial standing may be assessed by reference to whether the ASDE has sufficient and

reliable financial resources to maintain vehicles, implement software updates, respond to regulatory demands and satisfy penalties or redress orders. Evidence may include audited accounts, solvency statements, insurance arrangements, and access to contingency funding.

This extends across the whole lifecycle of the ADS and includes responsibilities for safety, updates, compliance and incident response.

In operator licencing, an operator will also need to show evidence of long term organisational stability. In operator licencing, guidance on suitable methods of finance are detailed within Statutory Document 2[1].

Because AV safety obligations extend over the entire operational life of the vehicle, regulators will expect assurance that the ASDE is a stable and sustainable entity, including:

- Audited financial statements
- Cash flow resilience
- Long term business viability
- Suitable insurance cover

This should be sufficient to protect against scenarios where a company collapses and leaves its fleet unmanaged.

Evidence of acceptable finance is covered within Statutory Document 2 and the calculations therein.

Question 13: In your view, what should be considered when assessing whether an ASDE is capable of competently discharging authorisation requirements?

Competence may be assessed through the ASDE's safety management system, technical expertise, governance structures and operational capability. Factors may include qualifications of key personnel, systems for monitoring AV performance, incident management processes and evidence of continuous improvement. Another consideration could be disaster recovery management.

Question 14

No response given.

Question 15: In your view, what, if any, additional information should be captured on the register of authorisations?

The register of authorisations needs to be centralised, transparent and easily available to the public. It should record key information, including:

[1] https://www.gov.uk/government/publications/traffic-commissioners-finance-march-2019/statutory-document-2-finance

- vehicle and system IDs
- the scope and limitations of each authorisation (including ODD)
- details of the ASDE and responsible individuals
- validity periods
- compliance history
- incident records
- any applicable conditions or restrictions

Linking in with operator licencing, the register of authorisations should be further expanded particularly with regards to:

- Technical safety information
- Software/feature versioning
- ODD limitations
- Data and cyber security compliance
- ASDE & NUICO accountability structures
- In use monitoring and incident learning indicators

Operator licencing provides:

- Clear responsible entity identification
- Transparency about the scale and scope of operations
- Public visibility of compliance responsibilities
- A means for enforcement bodies to trace operators

These principles remain valuable for AVs.

Question 16: How might you expect to use the information available within the register of authorisations?

The register would support regulatory oversight, enable effective information sharing between agencies, and improve transparency for insurers, law enforcement and the public.

Users of the register could rely on it to verify the eligibility and compliance status of particular vehicles or operators, inform insurance or policy decisions, and assist in coordinated incident response.

Publication of the information could be used as a means of increasing transparency and further building consumer confidence.

Question 17: In your view, what should be considered when developing the authorisation procedure?

The authorisation procedure is particularly important as correct design and operation of it will

be crucial to improving the likelihood of safe implementation of AVs, successfully investigating anything that goes wrong, improving the claims process for injured parties and further developing public confidence in ADS.

The authorisation process should be structured in stages, with clear timelines, opportunities for review or appeal, and ongoing engagement with stakeholders. This ensures the process remains adaptable to technological developments and insights gained from operational experience.

A robust change management process is essential, given the dynamic and developing nature of ADS software and functionality. Any significant update that alters safety performance, operational boundaries, or compliance should trigger a formal review and, where appropriate, reauthorisation. Minor updates should be recorded and made available for regulatory scrutiny, with clear documentation to ensure long-term traceability and accountability.

Compliance obligations, including costs and administrative requirements, must be balanced against the benefits of improved safety outcomes, reduced incidents, and increased public confidence. These requirements should remain proportionate to risk and be subject to regular reassessment as technology and operational contexts evolve.

A light touch approach to authorisation of ADS must be avoided. Such an approach, as seen in the United States, has resulted in many avoidable incidents, including deaths, injuries and damage to property. As a result, the National Highway Traffic Safety Administration (NHTSA) has had to conduct a series of expensive, time-consuming investigations, and the media and public have adopted a sceptical view of AV-related incidents, even when it was proven that the AV was not at fault. Such scepticism amongst UK consumers would hinder public acceptance of ADS technology and slow the safety gains it would provide by maintaining an unnecessarily high number of human-caused incidents and injuries. This would place more pressure on emergency services and the NHS.

Question 18: In your view, are there lessons from other regulated areas that should inform the authorisation regime, and why?

One of the best examples where lessons can be learned can be found in the Civil Aviation Authority. The CAA is a good example of authorisation, licencing, maintaining standards post-deployment and managing the requirements for those involved in the sector. This final point will be relevant when addressing requirements placed on ASDEs and NUICOs.

Lessons can also be learned from the Information Commissioner's Office, especially as it pertains to data collection, storage and sharing – points that will be particularly important when looking at AV-related incidents.

In an effort to increase public confidence in authorised bodies, an AV regulator could adopt a rating system akin to the hygiene rating used for restaurants.

Question 19: In your view, what processes should be in place to ensure that authorised vehicles continue to meet the legal safety standard over time?

Unlike traditional vehicles, those with ADS will have the potential to change their capabilities and performance substantially with software updates. This was recognised by parliament and was one of the motivations behind requiring the installation of 'safety-critical' software updates within AEVA.

The regulations, or possibly the Statement of Safety Principles, will need to include details about what software updates are considered 'safety-critical', who is responsible for their installation, the amount of time they have to complete installation and what the penalties/repercussions are for failing to install in that time.

Post-deployment monitoring and checks will be necessary to ensure that AVs continue to meet legal safety standards. The vehicle must be able to substantively comply with the Statement of Safety Principles and regulatory authorisation. Means of monitoring this compliance will be necessary.

Issues around AV-related hardware are also potential causes for concern. In the event of the need to replace AV-related hardware, replacement parts must conform to OEM specifications and be capable of operation within regulatory standards. Secondly, any calibration must be performed to OEM specifications to ensure the safest possible use of ADS. A quick check on Google shows that there are several websites addressing the possibility of people recalibrating ADAS sensors without relying on authorised professionals. As concerning as the idea of amateur ADAS sensor recalibration is, the risks arising from amateur ADS sensor recalibration are potentially far worse. Any monitoring regime must make all efforts to eliminate this possibility.

One way of checking on AVs is by updating the MOT. The current MOT test regime only relates to the roadworthiness of the vehicle in general. A more rigorous roadworthiness test would be appropriate to ensure continuous promotion of vehicle safety.

This new MOT test would need to perform a check of the ADS (both software and hardware) to ensure they are operating correctly and do not contain any illegal modifications. A software check for malware, viruses, etc. would also be beneficial.

There are a few issues with relying solely on an expanded MOT system. Firstly, new vehicles are not required to receive an MOT until they have been registered for three years. A number of safety-critical software updates could have been required in that time. Secondly, and relatedly, once an AV is required to receive annual MOTs, there is still a possibility that safety-critical updates could take place that remain unaddressed for far longer than is allowable, for example if an update was available one week after a vehicle's MOT, it might remain uninstalled for 51 weeks.

An expanded MOT would provide a good backstop for AV safety, but other inspection/monitoring measures would need to be put in place to ensure updates are installed

in a timely fashion. The most cost-effective option for a regulator would be to pass responsibility to the ASDE/NUICO.

Insurers will need to be informed of any changes to vehicle status, including failure to update ADS software, termination of ADS subscriptions or failure by an operator to complete relevant training.

The needs of insurers in adoption of ADS will be paramount given the need for third party insurance on all AVs (as with all road-going vehicles). We address insurance and insurers' needs below, but defer to the ABI and its response generally on these matters.

Question 20

No response given

Question 21: What, if any, costs do you think should be taken into consideration when assessing the impact of authorisation standards?

See response to Question 22.

Question 22: What, if any, benefits do you think should be taken into consideration when assessing the impact of authorisation standards?

The creation and implementation of authorisation standards must focus on the principle of 'safety-first', especially when ADS is in its infancy.

An abundance of caution will result in costs, sometimes significant ones, and CCAV is right to want to understand the costs and benefits of these. Safety, however, cannot be compromised in an attempt to lower costs at the outset; the opposite approach should be adopted at this early stage.

The authorisation standards that come out of this call for evidence must be drafted with the focus entirely on safety and the costs of that safety should be a secondary consideration. These safety gains, regardless of initial costs should be the focus, which will in turn build public trust and lower costs in the longer term.

Post initial deployment of AVs, with real world experience, the areas where regulations have demonstrated an overabundance of caution will become evident. The government can then relax those requirements, reducing costs only when it is safe to do so. The alternative is having to strengthen regulations after unwanted incidents, which would increase costs for compensators and damage public trust in ADS at a time when building trust is critical. This is what we are seeing in the US with both AV schemes and deployment of ADAS that is close to ADS, such as Tesla's FSD.

The benefit of this course of action is that public acceptance of these technologies is likely to grow more quickly as fewer incidents result in a relaxation of media scrutiny. As the public is

exposed to more AVs its trust in the safety of the technology will grow. This trust will be further strengthened by continued improvements in ADS.

If the government fails to inspire public confidence in ADS, take up will be limited. This, in turn will adversely impact the safety benefits that will be derived in the longer term from these new technologies. Conversely, a failure to adhere to the 'safety first' approach could lead to incidents involving ADS that would cause the media and public to turn against the technology, setting back mass market engagement by many years. It would also likely result in more incidents, increasing costs for compensators, emergency services and the NHS.

Question 23

No response given.

Question 24: What evidence, if any, can you supply on the ability of a driver to safely resume control after disengagement from driving tasks? No personal information should be provided as part of the evidence.

Studies going back to at least 1982 suggest that, in general, the less involved a human operator has to be in the operation of a machine, the greater the likelihood that the operator will have difficulty re-engaging with operating the machine and the longer it will take for the operator to re-engage.[2]

In a 2013 study, researchers found that resumption of manual control (in terms of steering behaviour in particular) continued to be erratic for up to 40 seconds after the transfer of control.[3]

Transition demands should be governed by scenario-based protocols, performance standards, and thorough validation in both real-world and simulated conditions, paying close attention to edge cases and high-risk scenarios.

Many AV trials have already been conducted across the UK and the information provided should be fully considered and factored in to any decision on this issue.

Question 25: In your view, should there be specific training for a UIC?

See response to Question 27

Question 26: What, if any, knowledge and skills outcomes should the training provide?

See response to Question 27

[2] See: L Bainbridge, 'Ironies of Automation', IFAC Proceedings Volumes, 15.6 (1982), pp 129-135.
[3] See, e.g., N Merat et al, 'Transition to manual: Driver behaviour when resuming control from a highly automated vehicle', *Transportation Research Part F: Traffic Psychology and Behaviour*, Vol 27, Part B (2014), pp 274-282, which found that resumption of manual control (in terms of steering behaviour in particular) continued to be erratic for up to 40 seconds after the transfer of control.

Question 27: In your view, how frequently should UICs undertake training or tests of their ability?

The ABI has published *Defining Safe Automated Driving*[4], a document setting out twelve key criteria for safe adoption of automated driving in the public sphere.

In addressing driver training and education, *Defining Safe Automated Driving* states that: 'Vehicles must ensure and validate that drivers understand the system functionality and their roles and obligations in automated driving before automation can start.'

We interpret that to mean that driver education needs to include the following:

1. Driver education on ADS must be compulsory. Drivers cannot activate ADS until they have completed the training; and

2. Each driver needs to complete the training. The vehicle needs to detect if there is a new driver and will then require completion of the training.

In addition, we believe the following would be beneficial to safe use of ADS:

- Training should be in the ADS-equipped vehicle, via the infotainment system, with the vehicle's sensors and inward facing cameras checking to make sure the driver is engaged with the training session;
- To ensure that drivers are kept up-to-date with changes to the ADS as they are improved, ADS-equipped cars should require refresher training courses. These do not need to be as comprehensive as the original training session;
- Just as the DVLA recently incorporated use of satnav in the driving test, we believe that it would be beneficial to include ADS in the driving test in the next few years.

Manufacturers, government and insurers need to work together closely to ensure that the training and education that drivers receive is clear, adequate and maximises the likelihood that all drivers who choose to use ADS will do so safely.

Manufacturers' primary role will be to develop the necessary training element, provide it via the vehicle's infotainment system, and ensure that all drivers complete the compulsory training before they can engage the ADS.

Defining Safe Automated Driving states: 'The [training] system must be inherently simple and intuitive to understand such that the need for training is minimised.' Manufacturers will need to bear this in mind when they develop their training systems.

Government's role will be to set mandatory training standards, oversee compliance and regulate for failure by ASDEs to comply. It will need to ensure that all training is compulsory for all drivers.

The frequency and content of training, as well as any associated costs and benefits, should be

[4] https://www.abi.org.uk/globalassets/files/publications/public/motor/2019/defining-safe-automation-technical-document-aug-2019.pdf

aligned with the need for effective, safe interventions without imposing impractical burdens.

We strongly urge government to consider updating the driving test to incorporate ADS as a component. Insurers need to set out in greater detail their requirements for training standards so that manufacturers and government know what will satisfy insurers' requirements and guarantee ADS-equipped vehicles are insurable, preferably at reduced risk and lower premiums when compared to non-ADS-equipped vehicles.

Question 28: How should a UIC be informed of any changes to the vehicle's authorisation?

A change to a vehicle's authorisation is a matter that affects a number of individuals and organisations. The UIC needs to be notified, but others also need notification, including the vehicle's insurer and DVLA.

The UIC should be notified at their registered address and via a notification system within the vehicle itself, probably using the infotainment system. The vehicle's insurer also needs to be notified. This is especially important as AEVA will not pertain to a vehicle that is no longer authorised to drive itself. The RTA will become the applicable act, and liability for damage to third parties will shift from the insurer back to the operator. Insurers need to know when this occurs. This is especially true if manufacturers are allowed to provide ADS services on a monthly subscription basis.

The possibility of a change to vehicle authorisation points to a wider need: a maintained vehicle-specific public registry or database that insurers, licencing bodies and members of the public can access to see if a vehicle is authorised to drive itself; something similar to the MOT history check available at https://www.check-mot.service.gov.uk/.

Question 29: In your view what, if any, costs do you think should be taken into consideration when assessing the impact of UIC regulation?

See response to Question 30.

Question 30: In your view what, if any, benefits do you think should be taken into consideration when assessing the impact of UIC regulation?

We refer you to our responses to questions 21 and 22 above. The logic that applies to a cost/benefit analysis of setting authorisation standards applies equally to UIC regulations.

Question 31: In your view, should there be a stated value expected for a transition period duration akin to UNECE Regulation No. 157?

See response to Question 33.

Question 32: In your view, what should the minimum value be, and why?

See response to Question 33.

Question 33: In your view, should different scenarios require different transition demand protocols, and why?

On a general level, we are opposed to a generally applicable minimum transition period of 10 seconds, as has been suggested repeatedly and is the minimum amount of time required under UNECE regulation 157 (5.4.4.1).

If a UIC is to be expected to evaluate a situation and retake control of a moving vehicle in 10 seconds, s/he needs to have been monitoring the DDT, at least to some degree, even when not responsible for the DDT.

We agree it is compatible with self-driving to require the UIC to respond to a clear and timely transition demand. We reiterate the importance of a 'safety first' approach.

There are a number of potential factors that will influence the amount of time it will take for a UIC to regain situational awareness having been distracted from the dynamic driving task. Whilst there is a lack of real world data (i.e. other than under artificial test conditions), an arbitrary allowance of 10 seconds is very likely to be insufficient.

In a 2013 study, researchers found that resumption of manual control (in terms of steering behaviour in particular) continued to be erratic for up to 40 seconds after the transfer of control.[5]

If the UIC is not involved in the driving process, because s/he is allowed to engage in secondary tasks, s/he will not have detailed knowledge of the current situation when an incident that requires his/her attention arises. Studies have made it plain that the majority of people who want AVs would use the technology so that they could engage in two activities: using their mobile phones and sleeping. In either case, and especially the second, bringing drivers back into the loop so that they are able to safely resume control of the vehicle will take longer than 10 seconds. This will be especially true given varying factors, including:

- Weather
- Ambient lighting
- Road type/conditions
- Type of vehicle
- Whether the AV can perform a minimal risk manoeuvre given the circumstances

[5] See, e.g., N Merat et al, 'Transition to manual: Driver behaviour when resuming control from a highly automated vehicle', *Transportation Research Part F: Traffic Psychology and Behaviour*, Vol 27, Part B (2014), pp 274-282, which found that resumption of manual control (in terms of steering behaviour in particular) continued to be erratic for up to 40 seconds after the transfer of control.

One of the benefits of this level of technology is that issues like duration of transition period can/should be written into the code that controls the ADS. For this reason, there is no need to rely on blanket simplicity.

Question 34: In your view, should the nature of a transition demand vary depending on the user-in-charge and why?

The Department for Transport is currently consulting on the possibility of introducing extra measures that young and novice drivers have to satisfy due to their lack of experience. The point is to increase overall road safety and reduce the number of incidents involving these drivers.

Recognising that at the outset all drivers will not be familiar with ADS it would be advisable to require a longer transition demands be adopted, as the technology beds in, it will be possible to reduce transition demand periods for those drivers who are more experienced.

It should be possible for vehicle manufacturers and ASDEs to adapt a vehicle's software to personalise requirements; just as modern vehicles can alter dashboard configurations, activation of certain ADAS features, etc via the multiple driver profile settings.

Question 35: In your view, should standards be established for transition demand interfaces across different vehicle makes and models, and why?

At the start of 2022, the Highway Code was altered to include the hierarchy of road users. The more harm a vehicle can cause other road users places it further down the hierarchy. Regulations that control transition demands need to recognise that these vehicles lower down the hierarchy are larger, heavier and generally take more skill to operate.

When ADS becomes widely deployed, we expect to see automated HGVs and buses/coaches. These vehicles are at the absolutely bottom of the hierarchy. They take longer to stop, require larger spaces for emergency manoeuvres and are likely to cause much greater harm to other road users (and passengers in the case of buses and coaches) if the operator fails to successfully regain control of the vehicle.

Because of this, the larger / lower down the hierarchy a vehicle is, the longer the required transition period should be.

Questions 36-37

No response given

Question 38: In your view, what capabilities should NUICOs generally possess to be able to adequately detect problems arising during NUIC journeys?

See response to Question 39.

Question 39: In your view, what capabilities, if any, other than remotely assisting the ADS and driving the vehicle, should NUICOs generally possess to be able to adequately respond to problems arising during NUIC journeys?

NUICOs must be required to insure their vehicles to a degree that provides appropriate compensation to third parties.

Supervise vehicles – This is essential to ensure the safe and continuous flow of traffic where a NUIC vehicle carries out a minimal risk manoeuvre or is involved in a collision.

Report incidents – In order to promote the safe operation of NUIC ADS, we think that the obligation should extend to the reporting of 'near misses', which requires defining. We recommend putting incidents into some context, by obliging operators to report all miles travelled, split by reference to the specific operational domain. All incidents should also be reported by reference to operational domain.

Take reasonable steps to safeguard passengers from assault, abuse or harassment. Absent a driver, placing an obligation on operators to adequately safeguard passengers is an absolute necessity to ensure consumer confidence in NUIC ADS.[6]

Potentially, there will be difficulties arising from the general duty to ensure passenger safety, especially given the absence of a user or user-authorised supervisor in the NUIC vehicle. How will an operator protect passengers from fellow passengers? What liability will they have if a passenger causes harm to a fellow passenger? What steps will they have to take to demonstrate that they took all reasonable steps to ensure passenger safety? How will 'reasonable steps' be determined?

The use of 'stewards' in NUIC vehicles would inevitably reassure, especially where the vulnerable passengers are concerned, provided that they have undergone the necessary criminal checks. Whilst stewards may be necessary initially to instil confidence, their use in private hire NUIC vehicles should not be mandated in the medium to long term, as it would somewhat undermine their purpose. On the other hand, there is no reason why constant CCTV (without audio) should not be mandated. Would CCTV effectively protect passengers? Would deployment of CCTV be deemed adequate reasonable steps to protect operators from liability or would further steps be required? How would those steps be determined?
Consideration should also be given to the positioning of 'SOS' or 'panic buttons' about the cabin which would put the occupant(s) in direct contact with the supervisor at the NUICO (and law enforcement services). Again, though, it is unclear if this would be considered reasonable or if more is required of the operator.

Question 40

No response given.

[6] See the finding contained in the CCAV commissioned report: *CAV public acceptability dialogue* (July 2019).

Question 41: In your view, what requirements, if any, should be put in place for NUIC vehicles which carry passengers in addition to the requirements in existing schemes?

In addition to the information contained in our answer to questions 38 and 39 above, we add the following.

For NUICOs providing passenger services, additional safeguards should include:

- adherence to all relevant safety and accessibility standards
- robust policies for crime prevention and incident response
- transparent data handling
- effective customer support
- an effective system for handling any incident, including a 'lessons learned' document which is shared with affected customers or the public generally

It is vital that NUICOs develop safety-first measures that provide the best possible protection for customers and responses in the event that an incident occurs. If potential customers do not feel safe using a service, consumer confidence will suffer, possibly affecting NUICO schemes more generally.

Questions 42 – 44

No response given.

Question 45: What requirements, if any, of the existing HGV operator licensing scheme should be disapplied, replaced or amended for HGVs operating under a NUIC operator's licence?

Traditional HGV operator licencing is built around human driver based operations, focusing on matters such as driver hours, tachographs, route compliance, operating centres and vehicle maintenance.

By contrast, NUIC operations rely on remote supervision, ADS behaviour, continuous fleet monitoring and software driven safety.

Therefore, many traditional requirements are ultimately not fit for purpose and should be disapplied, amended or replaced.

<u>Requirements that should be disapplied</u>

- Drivers' hours rules & tachograph requirements
    - *Replace with*: requirements for remote operator workload management and control room oversight, aligned with in use regulation.
- Driver defect reporting requirements
    - *Replace with*:

        - Mandatory automated defect detection system requirements.
        - Integration of ADS diagnostic alerts with NUICO control room.
- Speed limit compliance as a driver obligation
    - *Replace with*: requirement for evidence that ADS enforces legal speed limits (e.g. high-definition maps, sensor derived speed control).
- Driver competence / transport manager CPC requirements
    - *Replace with*: NUICO specific professional competence standards for AV operations

Requirements that should be amended

- Maintenance and Roadworthiness Obligations
    - *Amend to* include:
        - Software maintenance (over the air updates)
        - ADS calibration and sensor alignment
        - Cybersecurity patching schedules
        - Logging and audit of safety critical software changes
- Record keeping requirements
    - *Amend to*:
        - Require retention of ADS logs, fallback events, interventions, sensor faults, and remote operator actions.
        - Specify minimum retention periods for AV operational data.
- Operating centre requirements
    - *Amend to*:
        - Focus on ODD parameters rather than depot capacity.
        - Require evidence relating to geographic maps, road class permissions, environmental constraints.
- Notification requirements (material changes)
    - *Amend to* include:
        - Substantial ADS software updates
        - Cyber incidents
        - Changes to ASDE NUICO operational agreements
        - Changes affecting remote operation capability
        - Safety relevant map/ODD revisions

Requirements that should be replaced

- Professional competence (transport manager CPC)
    - *Replace with* NUICO specific competence requirements covering:
        - ADS behaviour
        - Human machine interaction
        - Remote operator training
        - Data management & cyber security
        - Incident response
        - Safety case governance

- Fitness/good repute tests based on driver-centric legal offences
    - *Replace with* AV specific good repute tests, focusing on:
        - Cybersecurity integrity
        - Ethical treatment of safety data
        - Accuracy of information supplied to regulators (a key Law Commission concern)
        - Responsible governance of ADS safety
- Safety assurance obligations
    - *Replace with*:
        - Continuous monitoring obligations
        - Safety case updates
        - Data reporting mandates
        - Participation in AV incident investigation learning loops

Questions 46 – 59

No response given

Question 60: What, if any, costs do you think should be taken into consideration when assessing the impact of NUICO regulation?
See response to Question 61.

Question 61: What, if any, benefits do you think should be taken into consideration when assessing the impact of NUICO regulation?

We refer you to our responses to **Questions 21** and **22** above. The logic that applies to a cost/benefit analysis of setting authorisation standards applies equally to NUICO regulation.

In addition, it is important that NUICO regulation take into consideration the potential benefits of the service to vulnerable customers, as well as potential risks to those same customers if the regulations do not provide adequate safeguards for their protection. Any harm suffered by vulnerable customers as a result will doubtless add increased costs for compensators and add extra strain to emergency services and the NHS.

Question 62: In your view, how can insurance play a role in ensuring that good financial standing of regulated bodies is met?

Insurance can support financial standing by ensuring that regulated bodies, and indeed non-regulated bodies, have access to funds to meet liabilities arising from collisions, defects, or operational failures. Insurance may also act as a financial safety backstop, reducing insolvency risk and supporting consumer protection. Insurance as a way to demonstrate financial standing is seen in the financial services sector, for example see: (1) Payment Services Regulations 2017, (2) the EU's Electronic Money Regulations 2011 and Directive (EU) 2015/2366, and (3) the EU's Markets in Crypto-Assets Regulation (MiCA).

Questions 63-67

As we stated in our General Observations, we fully support the ABI's submission to this call for evidence. We particularly endorse its responses to these questions.

We agree with the ABI that insurance must be embedded as a core component of the regulatory architecture from the outset. In particular, we support the ABI's position that clarity on liability, access to data, and alignment between authorisation, approval, and insurance requirements are essential to ensuring public confidence, effective redress following incidents, and the sustainable growth of automated mobility services.

Question 68: If insurers request vehicle data that goes beyond determining liabilities of incidents where an AV is directly involved in a collision, how could privacy and data protection requirements be managed?

Requests beyond core liability determination should be governed by strict data-minimisation principles and clear legal bases under UK GDPR. Safeguards such as anonymisation, access controls, and transparent notices to users can help balance insurer needs with privacy rights. The scope of such requests should be proportionate and subject to oversight.

Question 69: What, if any, costs do you think should be taken into consideration when assessing the impact of regulating the insurance of AVs?

We re-emphasise the points we raised in response to **Questions 21** and **22** above.

In addition, we note that costs may include investments in secure data handling systems of AV data, compliance resources, staff training, and adjustments to claims processes. Insurers may also face indirect costs where new data requirements necessitate IT upgrades or changes to underwriting models.

Question 70: What, if any, benefits do you think should be taken into consideration when assessing the impact of regulating the insurance of AVs?

We re-emphasise the points we raised in response to **Questions 21** and **22** above.

Regulating the insurance of AVs could improve consumer protection, or at least adopt a consistent minimum standard, and efficient claims handling.

Question 71

No response given.

Question 72: In your view, how might a regulated body determine if an AV has committed a traffic infraction?

See response to Question 73.

Question 73: In your view, what should be taken into consideration in the submission of standardised information to the IUR, and why?

A number of different forms of data will be available to determine if an AV committed a traffic infraction.

The most obvious source of data will be the AV itself, such as dash camera footage, data relating to speed, braking, steering input and GPS data. This is why we fully support incorporation of the ABI's *Automated Vehicles: Data Sharing Principles*[7] into the regulations that come out of this call for evidence.

Insurers have, after long consideration, developed a list of the types of data produced and recorded by AVs that will be necessary for them to be insurable. Many of these same data points will be useful in determining whether an AV committed a traffic infraction.

It will be necessary for authorities to require data owners to hand over the required data in a timely fashion and in a standardised form that is reasonably easy to analyse and, if necessary, interrogate.

There are other sources of data that will be useful in determining whether an AV committed a traffic infraction, including the evidence of the UIC and any independent eye witnesses. The regulated body should also have the power to seize CCTV footage that may have captured the alleged infraction. Consideration will need to be given as to whether or not the vehicle was operating within any applicable design or environmental parameters.

This data will become more widely available as the road network infrastructure advances, including smart and connected infrastructure.

It is crucial that the accuracy and consistency of the standardised information that is submitted to the IUR can be verified.

Question 74

The investigation and analysis of an alleged infraction or relevant incident is likely to be far more complex and involved than conventional RTC investigations. Specialist knowledge in relation to software and hardware capabilities, the ability of the vehicle to perceive and react to a hazard or emerging incident, and the ability of the UIC to take over control of the vehicle will all form part of the investigation. At present, we find that police investigations into serious or fatal RTCs are typically taking 18-24 months to complete and in some instances, much longer. The complexity of investigations relating to AVs could mean that IURS investigations take longer still.

[7] https://www.abi.org.uk/globalassets/files/publications/public/motor/2024/data-sharing-principles-for-avs.pdf

Question 75: What records, if any, should be retained regarding the maintenance and repair history of AVs?

The following records should be kept, either on paper or electronically. Proof of::

- Timely installation of all safety-critical ADS software updates
- Subscriptions and expiry periods of ADS-related technology (if applicable)[8]
- Installation of OEM-equivalent ADS hardware and calibration by licenced/qualified technicians (if applicable)
- Re-calibration of hardware by licenced/qualified technicians (if applicable)
- Passing a revised MOT that tests ADS hardware and software (see response to **Question 19** above)

Question 76: In your view, what specialist knowledge or handling, if any, will be necessary in order to preserve evidence, and why? If 'yes', what specialist knowledge do you think may be needed to preserve evidence, and why? Do not provide any personal information relating to yourself or another identifiable person.

Specialised knowledge of digital forensics, secure data extraction, and handling sensor logs without altering metadata may be required. Technical imaging tools may also be required (similar to imaging servers). This may maintain integrity in the evidence.

Question 77: Beyond the primary purpose of supporting an investigation what, if any, other purposes do you think a thing seized could be retained and used for?

Seized items may contribute to safety research, standards development, or training, provided privacy and commercial sensitivities are protected.

Question 78: What challenges, if any, are you aware of regarding access to data relevant to investigations?

Similar to challenges around telematics data, the main issue will be around proprietary ownership of data, and its format, and any special way to access it.

Question 79: In what circumstances, if any, would you consider it acceptable that the thing seized is delivered to someone other than the owner?

It may be appropriate to deliver seized items to law enforcement (or their associate) in their appropriate investigation in the same way that other property may be seized for the purpose of investigating criminal activity. In addition, authorised experts, forensic laboratories, or regulatory bodies where necessary. There should always be a lawful basis for delivering a seized 'thing' to anyone other than the owner.

[8] Tesla has stopped offering FSD purchase in the US and now requires a $99/month subscription to use the service: https://www.cnbc.com/2026/01/14/musk-tesla-full-self-driving-subscription-fsd.html

We consider would it acceptable that the thing seized is delivered to someone other than the owner if it is necessary to help prevent the risk of death or injury occurring in similar circumstances in the future.

Question 80: Beyond those already used for electric and hybrid vehicles, what other considerations, if any, do you think should be implemented during the destruction of an AV?

See response to Question 81.

Question 81: What considerations, if any, in addition to those for conventional vehicles do you think are appropriate for the storage of a seized AV?

In terms of data, personal data and special category personal data should be wiped from any AV, including any access to cloud-based storage facilities.

Question 82: In your view, what are the circumstances in which a seized AV should be sold rather than disposed of?

See response to Question 83.

Question 83: In your view what, if any, considerations are there in how an AV should be appropriately disposed of compared to a conventional vehicle?

The main point that we want to emphasise in our answer to these questions is that all required data that can be extracted from an AV needs to be extracted before that vehicle is destroyed, seized, sold or returned to the owner/operator.

This needs to be done in a timely manner to improve the speed of the claims process, and the data must be stored in a way that makes it shareable with and analysable by relevant parties.

Question 84: What information can you provide, if any, of existing sanctions regimes in other areas which take a similar, flexible approach to applying noncriminal sanctions?

While not a sanction, coroners are under a duty to make reports to a person, organisation, local authority or government department or agency where the coroner believes that action should be taken to prevent future deaths. The recipient of such a report will have 56 days in which to respond to confirm what action, if any, they are taking to reduce the risk of death occurring in similar circumstances in the future.

We are aware that many organisations are anxious to avoid being the recipient of such a report because of the reputational damage they can cause.

Question 85: In your view, what factors relating to an incident or traffic infraction would warrant the IURS to:
• issue a regulatory sanction under the AV Act, as opposed to a civil sanction?

• vary an automated vehicle's authorisation conditions, rather than suspending the authorisation altogether?
• issue a monetary penalty notice instead of a compliance notice?

The applicable sanction should of course be proportionate to culpability. Under present law it does not automatically follow that the most serious outcomes, i.e. death or serious injury, will result in the most serious outcome for a driver, i.e. an immediate custodial sentence. While the harm caused by the incident or infraction should properly be taken into account, it should not be the consequences of the incident that determine the gravity of the sanction, rather it should be culpability.

The gravity of the punishment could increase for particularly egregious breaches or evidence of deep rooted, systemic failings as opposed to one off or isolated incidents.

Question 86: In your view, should a regulated body's turnover be taken into account when setting the maximum limit for monetary penalties? If 'no', why not? If 'yes', how should turnover be calculated and why? No personal information should be provided as part of the evidence.

We would agree that a regulated body's turnover be taken into account when setting the maximum limit for monetary penalties. This will help ensure a degree of consistency and proportionality. For criminal offences the level of fine imposed on an individual will be determined by the gravity of the offence and their weekly income. Ranges can go from 25% to significantly higher[9]. We would recommend the adoption of similar principles here.

Questions 87 – 93

We do not agree that there should be any pre-determined upper limits for penalties. Penalties need to act as a means of encouraging ASDEs and NUICOs to engage in best practice, and so should be a percentage of a company's turnover. An upper limit that would severely punish a smaller company could be seen as an inconvenience that has to be factored into a cost-benefit analysis by a larger company.

Penalties should be proportionate to reflect the level of potential harm that could have resulted from the infraction. Repeat infractions or a seeming disregard for the penalties should result in more severe penalties.

A disregard of regulations by an ASDE or NUICO has the potential to cause real damage to the public's trust in ADS technology. We have seen examples in the US where vehicle manufacturers have refused to co-operate with regulators and investigators about data sharing[10], and the result has been largely negative in the media and from consumers.

The IUR should be in regular communication with ASDEs and NUICOs to ensure they

[9] See https://sentencingcouncil.org.uk/supplementary-information/approach-to-fines/
[10] See eg - https://edition.cnn.com/2025/10/13/business/tesla-self-driving-regulation. We accept that this is relation to ADAS rather than ADS but the principle remains the same.

understand the need to abide by the regulations in both letter and spirit, but the IUR must also have the power necessary to act swiftly and decisively to prevent any actions that could harm public trust.

Question 94: What, if any, costs do you think should be taken into consideration when assessing the impact of the IURS?

See response to Question 95.

Question 95: What, if any, benefits do you think should be taken into consideration when assessing the impact of the IURS?

We refer you to our responses to **Questions 21** and **22** above. The logic that applies to a cost/benefit analysis of setting authorisation standards applies equally to the impact of IURS.

Additionally, we would note that an increase in reliance on data in relation to enforcement and infractions is likely to increase costs in terms of their storage, expert analysis, disclosure and the possibility of challenging admissibility / satellite litigation.

The reliance on data is also likely to increase delays relating to disclosure and expert analysis and due to challenges.

Question 96: In your view, what methods could be deemed an 'appropriate communication' between enforcement officers and AVs, and why?

As well as blue lights, sirens and hand signals, we would suggest that the use of any electronic signage should be considered to be an appropriate communication. These could be 'move over' signs that are seen attached to Highways Agency vehicles, and the use of red 'X' signs on smart motorways.

In examples across the US, AVs have shown that they sometimes fail to notice traditional means of indicating communication, such as lights and sirens. In January, the National Traffic Safety Board (NTSB) announced that it was investigating Waymo's ADS-equipped taxis after a recorded 19 failures to stop for school buses (a federal law) in Austin, TX since September 2025.[11] Use of electronic signage could reduce the likelihood of incidents like this in the UK.

Question 97: In your view, what opportunities, if any, are there for the statutory inspectors to learn from other safety critical industries?

We would encourage statutory inspectors to work closely with and learn from police forensic collision investigators whose job it is to attend fatal and serious road traffic accidents and then prepare detailed reports setting out how, in their opinion, a collision occurred. These reports will be used in any court or coronial proceedings that may follow.

[11] https://www.reuters.com/world/us-safety-board-opens-probe-into-waymo-robotaxis-passing-stopped-school-buses-2026-01-23/

The investigator will consider the witness evidence of all parties who were either involved in or witnessed the collision, any environmental factors such as weather conditions or issues with the road surface, any defects with the vehicle that could have caused or contributed to the collision and any physical evidence capable of confirming how the collision occurred.

Question 98: In your views, what opportunities and challenges are there to encourage data and information sharing across regulated bodies, regulators and other stakeholders (e.g. the police) to foster a no-blame safety culture?

Opportunities include improved early identification of risks. Challenges include concerns about liability exposure, protection of commercial information, and data privacy constraints. Clear legal protections and anonymisation mechanisms may help support a no-blame culture.

Question 99: In your view, should there be any limitations placed on an inspector's role and powers considering other safety-critical industries in the UK and internationally, and why?

Limitations may be needed to balance investigatory effectiveness with proportionality, privacy, and commercial confidentiality. Powers should be clearly defined and subject to oversight to avoid mission creep or undue intrusion into unrelated activities.

Question 100: In your view, should there be an oversight function to review the actions and decisions of the statutory inspectors to ensure that they are using their powers appropriately, and why?

An oversight mechanism may help ensure inspectors exercise powers appropriately and maintain public confidence in the framework. Oversight could focus on procedural fairness, proportionality, and adherence to statutory purpose.

Question 101: What safety themes, if any, can be learnt from international deployments of AVs, or AV pilots in GB?

See response to Question 102.

Question 102: In your view, how can lessons learned from investigations into relevant incidents be used to improve:
• the pre-deployment processes (e.g. approval and authorisation)?
• the general in-use safety of AVs to prevent future incidents?

Given the dearth of deployments of AVs internationally, we have extended our answer to include deployment of ADAS that is on the cusp of ADS – systems such as Tesla's FSD and the level 3 systems being tested in China.

USA

The US is the largest market for FSD. There are approximately three million Teslas with FSD

capabilities on America's roads. Last August, the NHTSA launched an investigation looking into why Tesla apparently has not been reporting crashes promptly to the agency as required by its rules. In October, the NHTSA opened a separate investigation into the safety of FSD technology generally on the back of 58 reported incidents of Tesla vehicles violating traffic safety laws while operating in full self-driving mode.[12]

One of the concerning points that has come out of the coverage from the US is that the NHTSA's ability to test vehicles and features before they are allowed on the road is limited by law and regulation.[13] This shows the importance of drafting the UK's AV regulations in a way that gives the regulators the powers required to maximise safety both pre- and post-deployment.

Another lesson that can be learned can be found in how the NHTSA investigates incidents. Minor incidents, where there is minimal damage to individuals or property, are handled and published thematically. Larger and more damaging incidents are analysed and reported on individually with a 'lessons learned' theme to each report.

It is important that these investigations be made public, as is the case with NHTSA investigations, to build the public's understanding of ADS's capabilities and trust in the technology.

China

A good example of effective AV regulation can be found in China. A single fatal crash involving a level 3 vehicle last year has caused a slowdown of approvals and a general re-examination of the safety requirements.[14]

Questions 103 – 107

No response given.

Questions 108 – 112

Limitations may be appropriate to protect personal data and commercially sensitive information. Retention should be limited to material necessary for statutory purposes, with secure storage and defined retention periods.

Mechanisms may include international cooperation agreements.

Guidelines may address secure storage of evidence and its location, preservation of metadata, and standards relating to imaging, logging and general control of evidence may be necessary.

[12] https://www.pbs.org/newshour/economy/u-s-opens-tesla-probe-after-more-crashes-involving-its-so-called-full-self-driving-technology
[13] https://edition.cnn.com/2025/10/13/business/tesla-self-driving-regulation
[14] https://www.independent.co.uk/tech/china-self-driving-car-crash-b2889924.html

Disclosure may be necessary to inform stakeholders of systemic risks, provided that confidentiality and privacy safeguards are maintained. Specific purposes should be clearly defined connected to public interest. There should be a mechanism to challenge and/or review disclosure as appropriate.

Clear rules may promote consistency and confidence in the investigation process. Retention should be proportionate and procedures for secure destruction ought to form part of the rules.

Question 113: What, if any, costs do you think should be taken into consideration when assessing the impact of incident investigation regulation?

See response to Question 114.

Question 114: What, if any, benefits do you think should be taken into consideration when assessing the impact of incident investigation regulation?

We refer you to our responses to **Questions 21** and **22** above. The logic that applies to a cost/benefit analysis of setting authorisation standards applies equally to the impact of IURS.

Costs may include specialised staffing, forensic tools, data handling systems, and administrative oversight. Industry participants may also incur compliance and reporting costs. As well as the direct costs associated with incident investigation regulation, such as staff training and deployment costs, consideration will also need to be given to the cost to those who are the subject of an investigation, such as the cost associated with a commercial organisation's vehicle not being on the road while it is being retained and the cost of their employees taking part in an investigation.

Additionally, we would note that an increase in reliance on data in relation to enforcement and infractions is likely to increase costs in terms of their storage, expert analysis, disclosure and the possibility of challenging admissibility / satellite litigation.

The reliance on data is also likely to increase delays relating to disclosure and expert analysis and due to challenges.

The most important benefit is, of course, the improvement to public safety, the reduction of the risk of similar incidents occurring in the future and ensuring that lessons are learnt. Thorough, prompt and effective investigations will help maintain the public's confidence in this fast emerging and quickly developing area. In the long term, by improving safety there will also be significant economic benefits to be gained as well.

Questions 115 – 120

Capabilities may include real time monitoring, intrusion detection, incident triage protocols, isolation protocols, and escalation pathways. NUICOs should maintain response plans and ensure staff are trained in cyber response procedures.

Reporting mechanisms should ensure prompt notification where incidents affect operational safety or system integrity. Timelines and thresholds should be clearly defined, similar to existing NIS or GDPR reporting frameworks.

Reports may include incident description, affected systems, initial risk assessment, response actions taken, and steps to prevent recurrence. Sensitive personal information should not be included in any reports unless strictly necessary.

Questions 121 – 125

No response given.

Glossary

ADAS – Advanced driver assistance systems
ADS – Automated drive system
AEVA – Automated and Electric Vehicles Act 2018
ASDE – Authorised Self-Drive Entity
AV – Automated vehicle
AVA – Automated Vehicles Act 2024
DDT – Dynamic driving task
FSD – Full Self-Driving. Tesla's level 2 driver assist; formerly called 'Autopilot'
GDPR – General Data Protection Regulation
IUR – In-use regulator
IURS – In-use regulatory scheme
NHTSA – National Highway Traffic Safety Administrator (USA)
NIS – Network and information systems
NUIC(O) – No user in charge (operator)
ODD – Operational design domain
RTA – Road Traffic Act 1988
RTC – Road traffic collision
UIC – User in charge

FOR FURTHER INFORMATION:

For further information, please contact:

Peter Allchorne
Partner, Head of Strategic Advisory
T: 0117 918 2275
E: pallchorne@dacbeachcroft.com

Michael McCabe
Solicitor
T: 020 7894 6315
E: mmccabe@dacbeachcroft.com

Joanna Folan
Legal Director
T: 020 7894 6350
E: jfolan@dacbeachcroft.com