BUS INDUSTRY CONFEDERATION
moving people

Preliminary consultation on Cyber Security and Software Update requirements

May 2026

Contents

The Bus Industry Confederation **3**
About Buses 3
Industry Snapshot | 2025 4
Executive Summary **5**
Response **6**
Survey feedback **7**
1. Adoption of UN R155 and UN R156 management systems: 7
2. Management system implementation in Australia: 9
3. Affected vehicles in supply: 10
4. General questions: 10
Contact **12**

The Bus Industry Confederation

The Bus Industry Confederation (BIC) is the national independent peak body for the Australian Bus and Coach Industry. We represent over 160 bus and coach operators, body, chassis and complete bus manufacturers and suppliers, parts and service providers, professional services, and state bus associations on issues of national importance.

Our membership is becoming increasingly diverse as key energy and infrastructure partners join as we transition the fleet to low and zero emissions. The BIC advocates on behalf of our members to federal, state and territory governments and associated bodies, to ensure the safe and efficient carriage of passengers, along with safe and sustainable operations and supply chains that support the industry.

About Buses

Buses serve as mass transit, delivering benefits like reduced congestion, lower pollution, and enhanced productivity, as well as providing critical social mobility through frequent local routes. These benefits extend to improved public health, lower crime rates, and better overall social outcomes, resulting in reduced costs for health and legal systems. The Australian bus industry is uniquely positioned to lead the transition to zero-emission technologies[1]. for heavy vehicles, assisting decarbonising strategy for the nation.

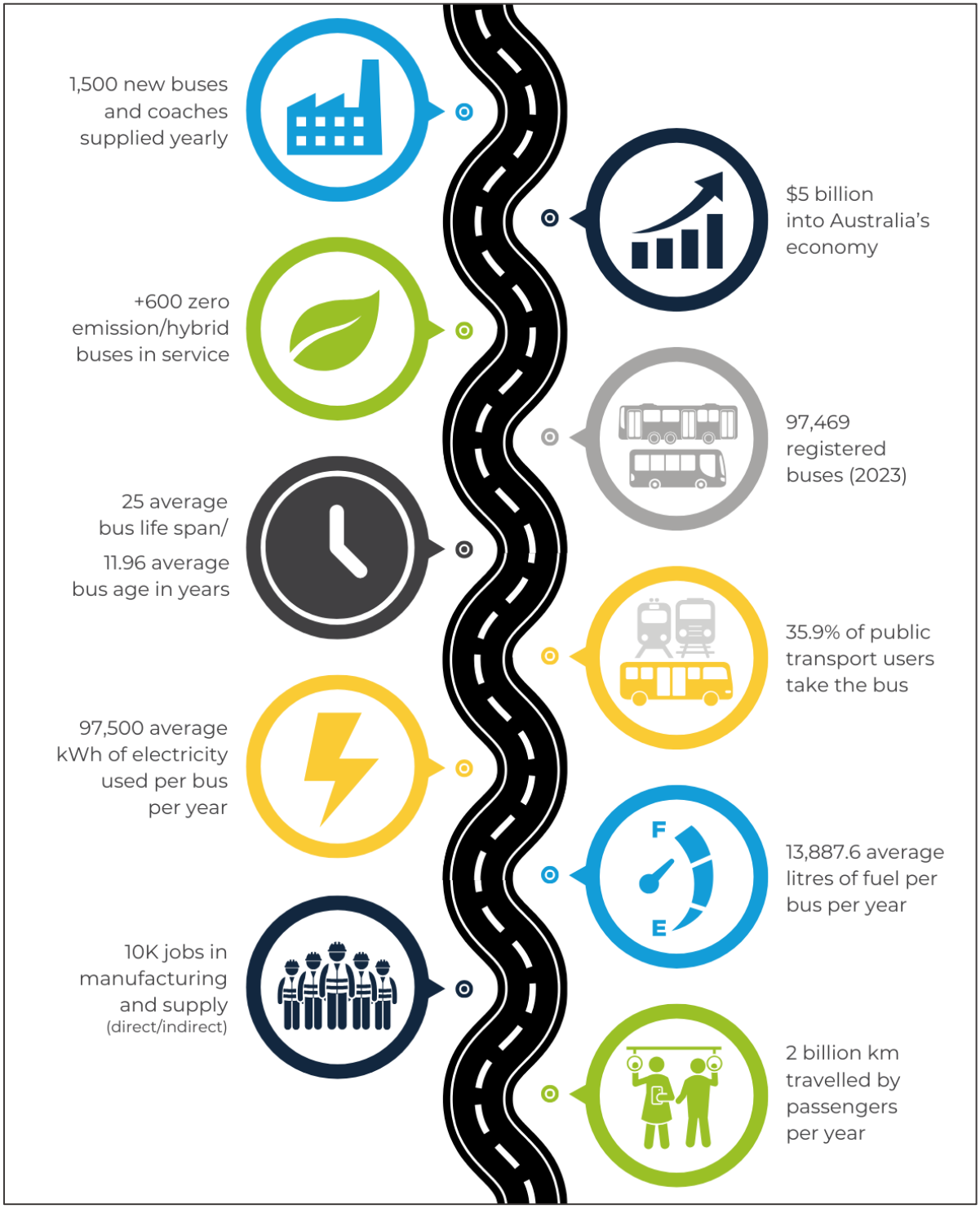
Buses have a strong and diverse manufacturing, and supplier presence in Australia providing 10,000 direct and indirect jobs in Australia. This encompasses full manufacturers, assemblers, importers, component manufacturers, suppliers, and importers. We provide an economic contribution $5Billion yearly to the Australian economy.

Buses provide a cost-effective safe role in moving people from and to their destinations every day, whether it is dense urban outer urban, regional, remote, or interstate. For example, in outer suburban areas, where other mass transit options are scarce, buses are vital in addressing poverty, disadvantage, and the financial strain of car ownership. They offer essential mobility to communities facing isolation, poor services, and socio-economic challenges.

Buses carry more people further than any other public transport mode.

[1] BIC Policy Paper – Driving Towards Zero Emissions

Industry Snapshot | 2025



Executive Summary

The Bus Industry Confederation (BIC) has previously supported and called for the introduction of the proposed cyber security regulations listed below via the Vehicle Standards Consultive Forum (VSCF).

- UN Regulation No. R155
  Cyber Security and Cyber Security management systems (CSMS)
- UN Regulation No. R156
  Software update and Software update management systems (SUMS)

Both the VSCF joint submission and this submission call for a nationally harmonised standard to avoid the bespoke requirements that some jurisdictions have already introduced or are in the process of developing. Fragmented, jurisdiction-based regulation carries a greater cyber security risk than a coordinated national approach and undermines the protections available to the Australian public.

The bus industry continues to broadly support the introduction of R155 and R156. This submission focuses on *readiness, timing, and harmonisation* as the critical considerations for successful implementation.

Separate approaches at a jurisdictional level for buses will be very difficult, prohibitively expensive to maintain and govern. This runs the very real probability of putting Australia at a greater national risk. **This must be solved at a national level.**

Recommendations

1. **Harmonisation**: Request jurisdictions to **pause on their own individual pursuits** on vehicle cyber security and instead **align with a national approach** even if the national process takes time to implement.

2. **Timing:** Allow a **minimum of three to four years** from the introduction of federal regulation for industry to prepare for the extremely complex compliance requirements. Timing should reflect a whole-of-automotive industry approach, recognising different levels of readiness from different sectors.

3. **Readiness:** In parallel with regulatory development, ensure Australia **has sufficient in-country testing capability and a suitably qualified workforce to meet and maintain regulatory requirements**. This includes investing in local infrastructure, building workforce capability for ongoing compliance and regulatory oversight, and supporting collaboration between industry, regulators, and training organisations. Although this may sit beyond DITRDCSA's direct remit, it will require close cross-government coordination so relevant agencies can prepare accordingly.

   Successful implementation depends on these foundations being in place.

4. **Guidance: Develop guidance materials** to help smaller suppliers transition to the new regulations. Given the complexity of compliance, including interactions with existing laws such as *right to repair*, tailored support is critical to help smaller suppliers (and larger suppliers where needed) **manage the transition and meet ongoing compliance obligations**.

5. **Local pathway:** With 60% of buses partially or completely manufactured in Australia, a local assessment and compliance pathway for a Non E-mark suppliers should also be accounted for.

6. **Cost:** All State and Territory governments, and the consumer need to be fully prepared for **cost increases to cover the implementation of and ongoing maintenance** of cyber systems. This is the consequence of protection.

   These costs need to be communicated strongly to states and territories so that they understand and account for price rises resultant of these changes.

7. **Alternate standards:** Consideration be given into permitting other equivalent standards for cyber security in addition to R155 and R156. Whilst the government strategy is to align with European regulations, the reality is that many suppliers are based in Asia or the Americas will wish to use other 'equivalent standards'.

BIC recommends DITRDCSA to advance a **nationally harmonised framework** for the bus sector and stands ready to work with the department and industry stakeholders to support practical, well-resourced, and achievable implementation across the sector.

Response

The Bus Industry Confederation welcomes the opportunity to provide input to the Department of Infrastructure, Transport, Regional Development, Communications, Sports, and the Arts (DITRDCSA) consultation on Preliminary consultation on Cyber Security and Software Update requirements.

BIC has previously indicated strong industry support to the proposed requirements, we surveyed a broad cross-section of the Australian bus supplier industry, providing insight into sector readiness and commentary. This is further to a similar survey conducted in 2023 following a previous consultation [2].

Figure 1- Brisbane peak hour showing importance on buses to move a city.

[2] https://bic.asn.au/wp-content/uploads/Cyber-Security-Submission-to-DITRDCA-Nov-2023-Final.pdf

Survey feedback

The following is a summary of the answers to the survey questions requested of DITRDCSA in preliminary consultation paper dated April 2026.

1. Adoption of UN R155 and UN R156 management systems:

Have you adopted the management systems that align with the principles of UN R155 and UN R156? For those based on overseas parent company processes, have these been specifically incorporated into Australian practices?

Many organizations have already adopted management systems aligned with UN R155 and R156, others are in progress, and a proportion have not yet begun. This spread is consistent with the global trajectory of the automotive industry.

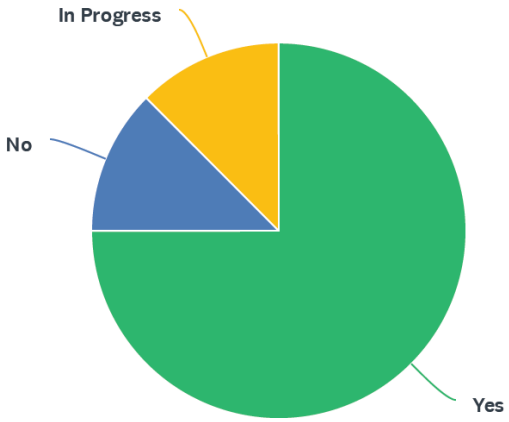


Figure 2 – General adoption of R155 and R156 for buses

From an Australian perspective, more than 60% of respondents suppliers indicated that they are in progress to adopt the standard. They also highlighted this is a complex task, especially in an environment where multiple jurisdictions are in essence setting their own requirements.

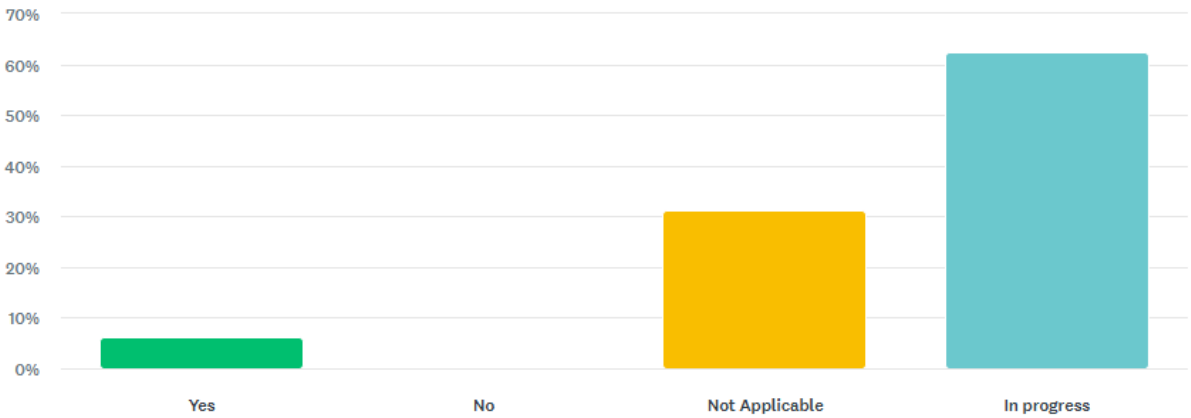


Figure 3 – Adoption of R155 and R156 in Australia for buses

If not, what management systems have been adopted with regards to cyber security and/or software updates to ensure safe vehicles being supplied to the Australian market?

Sixty-eight percent of respondents indicated they had already been required to implement varying cyber security standards as part of contractual requirements to provide buses in Australia.

Aside from UNECE R155 and UNECER155, the following standards were mentioned.

- Transport for NSW (TfNSW) Standards (Various).
- ISO 27001 (Information Security Management)
- ISO 21434 (Road Vehicle Cybersecurity Engineering)
- ISO 24089 (Road vehicles. Software update engineering)
- ACSC Essential Eight (Maturity Level 3)

There is also a proposal from TfNSW presently to enhance their own requirements based on their own existing requirements for other modes such as rail. They are:

- TfNSW TS 04990: Industrial automation and control systems (IACS), Overview
- TfNSW TS 04993: Risk management procedures for TS 04990.
- TfNSW TS 00031: Threat-Based Cyber Security Controls Part 1: Controls and Implementation Requirements

Where operators are required to procure vehicles or components across multiple states, differing standards create compliance complexity, increase costs, and may inadvertently weaken overall security position.

There was a strong industry preference for a harmonised approached moving forward.

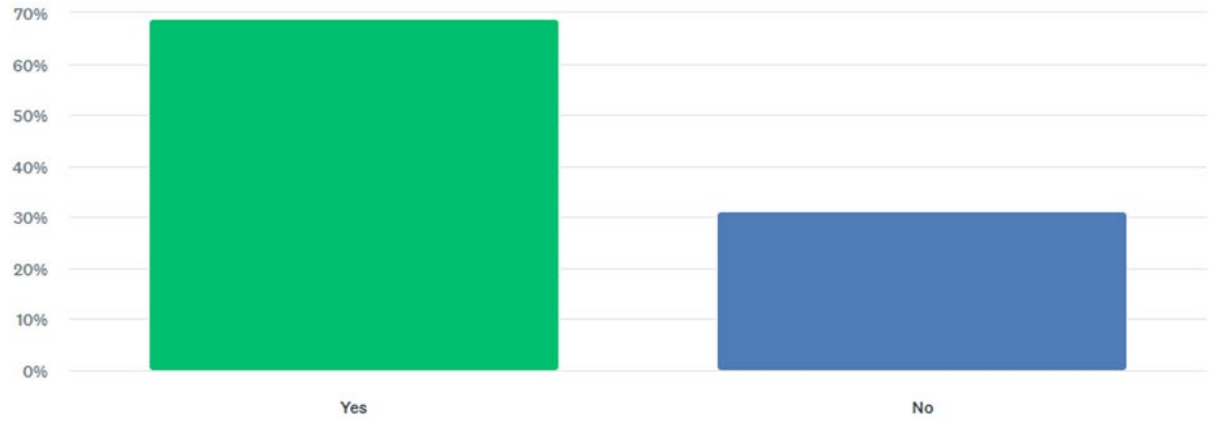


Figure 4 – Uptake of other cyber standards in Australia

2. Management system implementation in Australia:

Do you have trained staff in Australia to implement your cyber security and software update management systems, or is there a reliance on overseas staff?

There was a confident response to suppliers having support based in Australia with only 25% relying on overseas specialists as a primary support mechanism.

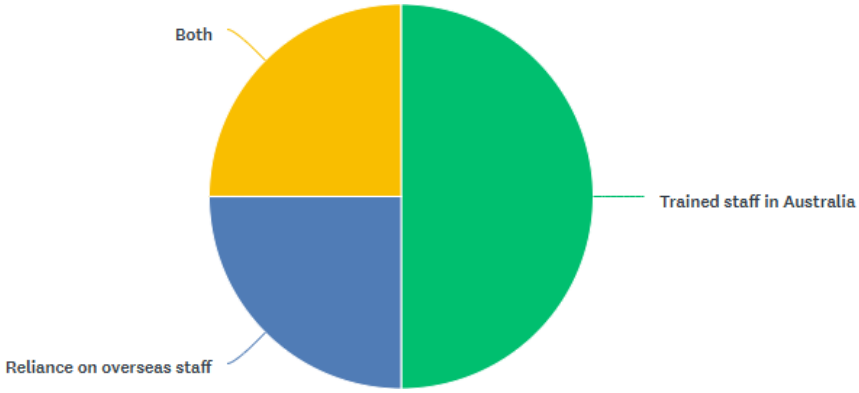


Figure 5 – Readiness of trained staff

This finding has two important implications for regulation:

- Organisations relying on overseas staff will need time to build or contract local capability to implement, monitor, and respond to CSMS and SUMS requirements on an ongoing basis. This is particularly relevant given the UN R155 requirement for lifecycle management of cyber risks.

- The development of a skilled local cyber security workforce in the automotive sector should be considered a complementary government priority alongside the regulatory framework.

How many cyber incidents have you identified in Australia, what type of incidents were these, and how did you respond to them? How many cyber incidents have you proactively identified in Australia, and what types of cyber incidents were these?

No respondent indicated they have been subject to a cyber-attack or one proactively identified. This isn't to say there isn't a risk, it just hasn't happened yet in our industry to our knowledge. However, preparation is far better than reacting after an incident.

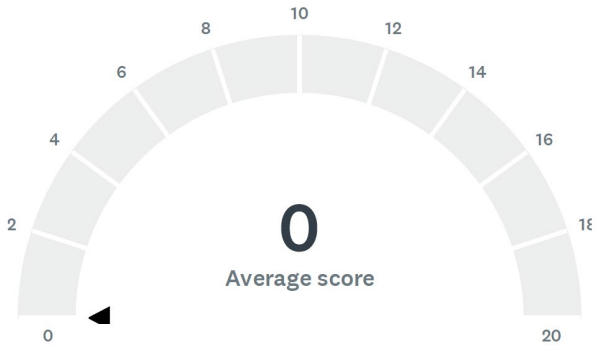


Figure 6 – Reported Cyber-attacks in Australia on buses.

3. Affected vehicles in supply:

What percentage of vehicles or components (covered by a CTA), which you have supplied to the Australian market are covered by your cyber security management system? What percentage of vehicles or components (covered by a CTA), which you have supplied to the Australian market are covered by your software update management system?

In both questions at least 50% respondents indicated full coverage whereas others indicated partial coverage at 50%. Overall, the industry average for coverage sits at 52.4%.

The nature of responses to these two questions reflected a structural divide in the industry between Suppliers with established global CSMS frameworks other suppliers that have not yet implemented formal cyber security management systems, possibly smaller or more specialized suppliers.

This is significant for policy design as those not covered represent organizations that will require the most support and the longest implementation timeline.

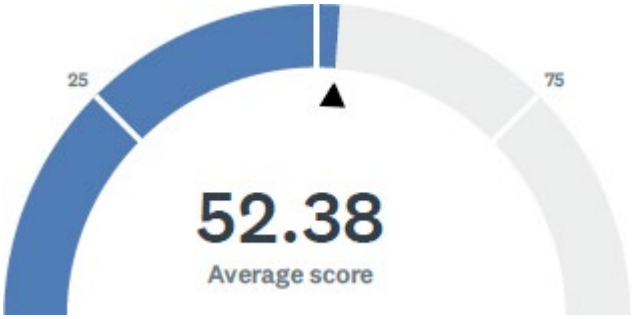


Figure 7 – Average of components/new vehicles covered by a management system

4. General questions:

If not already adopted, what would be the predicted costs for you to adopt UN R155 and UN R156 for vehicles supplied to Australia? And what would be the biggest challenge for adoption?

Answers to this question varied up to $800,000. A common theme is the additional cost of ongoing compliance which for a large supplier could be in the vicinity of $100,000 or greater per year. This will increase as the carpark of vehicles increase and the amount of administration also increases.

These figures indicate that the cost of compliance is not trivial, particularly for smaller component and technology suppliers. However, they also confirm that compliance costs are proportionate to the scale and complexity of the organization.

Consumers also should be aware of the cost of protecting such complex vehicles and despite the cost, protection to a global best practice standard is reassurance against possible attack.

Any additional comments?

Timing

In addition to the survey questions, we asked the following question:

> *If not fully cyber security compliant already, how long do you estimate it would take your organization to achieve compliance?*

Despite industry support, this is a key consideration given the complexity or implementing these proposed standards which industry supports.

Answers were again varied reflecting the diverse levels of readiness across the industry with 30% indicated a minimum of two years was required.

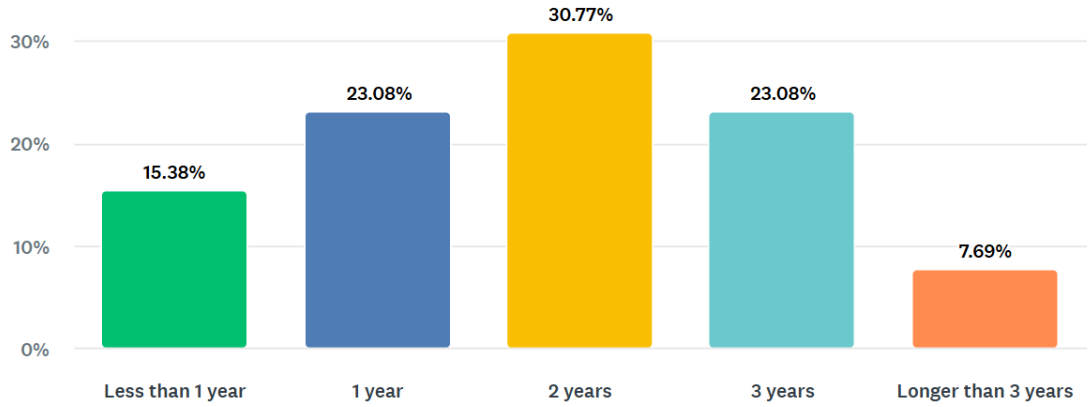


Figure 8 –expected time to attain compliance.

Imposing an unrealistically short compliance timeline risks excluding suppliers from the Australian market or creating a wave of non-compliance. Even with many jurisdictions imposing or in the process of implementing requirements, suitable implementation time is critical. This needs to be respectful of all the needs of all sectors, car, truck, bus, caravan, crane, and bike.

Other comments

Respondents' answers to *other comments* can be summarised as below

a) Harmonisation Across States and Territories

This is identified as the most significant challenge. Multiple respondents explicitly called for a single national standard as BIC has done, with one noting: *"Fragmentation will only increase the risk of cyber security attacks."* Federal leadership through ADRs is seen as the appropriate mechanism

One national standard administered by one national regulator, with states and territories to pause on their own automotive cyber agenda and co-ordinate nationally.

b) Learn from the European Implementation Experience

Respondents with European operations provided a valuable cautionary note that while the EU implementation of UN R155/R156, was broadly successful, it has involved significant interpretation challenges, elevated certification costs driven by annual audit requirements, and misalignment between CSMS/SUMS process front-loading and existing product liability frameworks. Australia has the opportunity to design a streamlined implementation that avoids these pitfalls.

Industry encourages DITRDCSA to consult directly with industry that have undergone EU type approval under UN R155/R156 when developing the Australian implementation guidelines.

c) **Testing Access and suitable people**
Access to accredited testing facilities is a practical constraint for manufacturers assembling vehicles in Australia, with available facilities currently limited. Government should consider whether establishing a register of approved Australian testing laboratories ahead of the regulation coming into force would be beneficial to industry, and whether international laboratory equivalence arrangements can be made. This could be facilitated under an approved test facility framework as per RVSA guidelines.

Readiness is critical for practical implementation capability.

d) **Workability and Repair Industry Implications**
Respondents noted that additional security layers may impact the workability of vehicles from a repair and maintenance perspective. This has implications for the broader automotive repair and service industry, which is identified as an affected stakeholder in the consultation paper. Government should ensure that CSMS and SUMS frameworks accommodate legitimate access for authorised repair, diagnostics, and software updates by repair and service industry.

e) **Engage Industry in the Development of Implementation Guidance**
Industry requests ongoing engagement through the Vehicle Standards Consultative Forum and other mechanisms as the ADR drafting and implementation guidance is developed. Early visibility of draft ADR text, proposed transition arrangements, and interpretation guidance and timing is essential to allow industry to plan and invest with confidence.

Contact

Dean Moule, National Technical Manager

T | 04124 990 956

E | dean.moule@bic.asn.au

W | bic.asn.au