



29 May 2026

Department of Infrastructure, Transport, Regional Development,
Communications, Sport and the Arts
Vehicle Safety Policy & Partnerships Branch, Road Vehicle Safety Division,
Vehicle Standards Consultative Forum

Emailed via: standards@infrastructure.gov.au

To whom it may concern,

Re: Federal Chamber of Automotive Industries submission to Preliminary Consultation on Cyber Security and Software Update Requirements.

The Federal Chamber of Automotive Industries (FCAI) welcomes the opportunity to provide the following feedback to the Vehicle Standards Consultative Forum, preliminary consultation on cyber security and software update requirements.

The FCAI is the peak industry body representing the Australian automotive industry. Its membership comprises manufacturers, importers and distributors of passenger vehicles, SUVs and light commercial vehicles into Australia.

Summary

The FCAI acknowledges the work which the Department have been undertaking to explore the adoption of global harmonised standards to address the increasing importance of cyber security and software updates in automotive vehicles today.

The preliminary consultation referenced two options:

- Option 1: Introduce new ADRs and implement RVS rule changes
- Option 2: Regulate under the Cyber Security Act 2024,

and specifically requested views regarding option 1 via a list of questions.

The FCAI's recommendation is that Option 1 is the optimal outcome to support the development and deployment of appropriate regulation. The introduction of new ADR's and implementation of RVS rule changes, with requirements harmonised with UN R155 and UN R156 would continue to align Australia with global best practice.

In contrast, adopting Option 2 would likely increase regulatory burden placed on automotive manufacturers through the addition of new regulators and development of policies which are not harmonised to international standards. Applying bespoke requirements under Option 2 would lead to increased costs associated with the design and development of vehicles, which would ultimately be passed on to the consumer.

The FCAI would note that Australia is a contracting party to WP29, and the implicit commitment to mutual recognition would not be honoured if Australia took a non-harmonised pathway to the development of new standards as suggested in Option 2.



To support the development of these responses the FCAI has continued to engage with members through the FCAI Technical Committee, and the feedback provided demonstrates that cyber security and software update processes currently applied in Australia vary in structure and approach.

In general, systems and processes which are in place align with UN R155 and UN R156 to varying degrees. The individual efforts of each OEM to develop their own cyber security and software update systems will be enhanced through regulatory clarity such as aligning ADRs with UN R155 and UN R156.

OEMs generally rely on centralised global teams or headquarters to manage cybersecurity and software update systems. Presently, as Australia has not implemented these regulations, local operations are often considered outside the scope of existing UN R155 and UN R156 approvals. As a result, Australian operations may not be fully integrated into the relevant global management processes.

The FCAI recommends adopting ADRs fully harmonised with UN R155 and UN R156 and applying supporting RVS rules.

To support the efficient implementation and administration of UN R155 and UN R156 it will be critical to ensure that the Department implements processes that allow for the;

- Acceptance of UN approvals including:
 - Certificates of Compliance (CoC) for Cyber Security Management Systems (CSMS) and Software Update Management Systems (SUMS)
 - United Nations Economic Commission for Europe (UN ECE) type approvals,
- Acceptance of management system certifications from recognised technical services,
- Recognition and acceptance of the associated auditing and reporting mechanisms,
- Avoidance of re-certification or duplicate assessments in Australia; and
- Provision of adequate lead times of 3 years for new models and 5 years for all models from final rule publication,

Additionally, timing for the implementation of new ADRs must continue to account for the established practices and processes which global OEMs conform to when looking at vehicle development, approvals processes, testing and training.



Consolidated responses to Questions:

Have you adopted the management systems that align with the principles of UN R155 and UN R156?

Overall, OEMs indicate broad adoption of management systems aligned with UN R155 (Cybersecurity Management System – CSMS) and UN R156 (Software Update Management System – SUMS), but with varying levels of maturity, certification, and geographic deployment.

FCAI members demonstrate a strong alignment with UN R155 and R156 principles, with many OEMs having established and certified systems. However, the scope of certified systems does not yet include Australia with full deployment focussed on regulated markets such as Europe and Japan.

Some OEMs have indicated that capability development in markets like Australia is linked to regulatory clarity. Once regulatory clarity is achieved, an implementation period of at least 3 years is needed where system architecture changes are necessary, along with further development of necessary management structures, resourcing and training.

For those based on overseas parent company processes, have these been specifically incorporated into Australian practices?

Feedback indicates that overseas parent company management systems aligned with UN R155 and UN R156 are not fully incorporated into Australian operations. In several cases, systems are only implemented in regulated markets such as Europe and Japan.

Some OEMs apply elements of global processes indirectly, such as:

- Internally equivalent processes to those defined by UN R155/R156. Local operations handle awareness and initial detection, while core cybersecurity and response functions remain centralised overseas.
- Utilisation of broader global processes, however not explicitly localised.

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?

While most OEMs have established global UN R155/R156-aligned systems, these are generally not fully implemented or localised in Australia. Instead, Australia is typically:

- Not presently included within the scope of UN R155/156 approvals,
- Supported directly or indirectly by global equivalent processes, or
- Operating under simplified or equivalent internal frameworks.

Full incorporation into Australian practices is largely dependent on future regulatory clarity.



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?

Most OEMs rely on centralised global teams or headquarters to manage cybersecurity and software update systems.

Critical functions such as incident detection, response, monitoring, and system governance are typically handled overseas.

A range of local support structures were described:

- In some cases, management systems are not implemented locally, making local training unnecessary at present.
- Local staff receive training for awareness and basic sensing, with advanced operational responsibilities managed via global head offices. Australia acting as a frontline or liaison rather than a control centre.
- A hybrid structure, with global teams leading cybersecurity and update management and local teams providing supporting technical input. External providers may supplement capabilities.

There is a general acknowledgement that local capability will need to expand as regulatory requirements increase.

Overall, there is a clear industry-wide pattern of centralised cybersecurity and software update management, with minimal in-country expertise in Australia. Local teams, where present, are typically focused on awareness and support, while core technical and operational responsibilities remain with overseas parent organisations.

Expansion of trained Australian-based staff is widely anticipated but contingent on future regulatory requirements, particularly the adoption of UN R155 and R156 into Australian law.

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

The OEMs that responded did not identify any cyber incidents.

How many cyber incidents have you proactively identified in Australia, and what types of cyber incidents were these?

The OEMs that responded did not identify any cyber incidents.

What percentage of vehicles which you have supplied to the Australian market are covered by your cyber security management system?

It was not possible to determine a specific percentage of vehicles, and there is some nuance in how 'covered' is interpreted.



Vehicles sold in Australia may be built on architectures or developed under processes aligned with UN R155, however, Australia itself is not formally included in certification scope, meaning coverage is implicit rather than officially recognised or declared as a percentage.

Generally, respondents interpreted this question in relation to coverage under a formally approved UN R155-aligned Cybersecurity Management Systems (CSMS). Responses included:

- Not covered under an 'approved' CSMS
- Partial or transitional coverage, with the transition aligned with new model launch schedules.
- Indirect, or platform-based alignment.
- Coverage under an equivalent framework.

While some vehicles benefit indirectly from global systems or compliant architectures, formal inclusion of Australia within the scope of an approved CSMS is generally not present yet.

Coverage is expected to increase progressively as newer, globally compliant platforms enter the market, with current implementation largely driven by overseas regulatory requirements.

What percentage of vehicles which you have supplied to the Australian market are covered by your software update management system?

Responses indicate that coverage of vehicles in Australia under Software Update Management Systems (SUMS, UN R156) is currently limited with most OEMs either not implementing SUMS locally or coverage is limited or emerging.

- Several manufacturers explicitly stated that vehicles in Australia are not covered by a formally implemented SUMS.
- Some respondents indicated partial or emerging coverage, with coverage expected to increase progressively as compliant models replace older ones.
- Several OEMs highlight that SUMS processes exist globally and are applied during development, however, Australia-specific implementation and certification is not yet in place.

While global SUMS processes are widely established, their formal application to Australian vehicles is limited. As with cybersecurity systems, expansion is expected to occur gradually through new model cycles and in response to future regulatory requirements.

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?

Respondents indicated that costs were difficult to estimate:

- Costs are highly variable and dependant on factors such as vehicle lineup, sales volume, and integration with global programs.



- Because cybersecurity and software update systems are embedded across the full vehicle development lifecycle, it is difficult to separate Australia-specific costs.

Lower incremental costs are expected where systems already exist:

- Core systems are already developed and deployed globally, meaning incremental costs would be required for Australia.
- These costs would mainly be administrative or procedural, such as:
 - Preparing market-specific documentation
 - Extending certifications (CSMS/SUMS) to cover Australia
- With no major technical redesign of vehicles.

Higher costs where Australia is not yet covered and/or vehicle systems are not yet compliant:

- If the Australian market is not already covered, adoption can be expensive and time-consuming, reflecting the effort to modify systems, processes, and support infrastructure.

Lead Time as a Critical Factor:

- A consistent theme is the need for sufficient implementation timeframes:
 - Typically, for new regulation at least 2 years is provided from final rule publication for new models and 4 years for all models, aligned with vehicle development cycles. However, feedback received from OEMs has indicated that the complexity associated with vehicle and management systems development, including approvals, necessitates a longer implementation timeline.
 - The FCAI would recommend that 3 years from the final rule publications would be appropriate for new models, and 5 years for all models would provide appropriate development timelines without restricting the earlier introduction by some OEMs. This is particularly important where electrical architecture requires upgrades.
 - The FCAI notes that this would only be appropriate for the full harmonisation of UN R155 and UN R156.
- Adequate implementation periods are seen as essential to minimise cost and disruption.

Key Challenges identified were:

1. Localisation and administrative requirements

- Adapting global systems to Australia may require:
 - Market-specific documentation and processes
 - Integration of local identifiers or regulatory variations
- Any unique Australian requirements could increase complexity and cost.

2. Coordination across global and local stakeholders

- Implementation requires alignment between:
 - Headquarters (global system owners)
 - Regional and local Australian operations



- Ensuring consistent governance while accommodating local needs.

3. Integration with vehicle development cycles

- Cybersecurity and software update requirements must be designed into vehicles from early development stages
- Retrofitting or late-stage adoption is complex and inefficient, reinforcing the need for adequate lead times.

4. Training and operational capability

- The need for staff training, ongoing capability development, and operational maintenance.
- This can be a key barrier in markets like Australia where local expertise is currently limited.

5. Regulatory uncertainty and alignment

- OEMs stress the importance of:
 - Harmonisation with existing UN regulations
 - Avoiding unique Australian requirements, which would increase cost and delays
- Acceptance of existing UNECE certifications is seen as critical for efficient adoption.

Conclusion

In conclusion, the financial impact of adopting UN R155 and R156 in Australia is generally expected to be moderate for OEMs with established global systems, and higher for those needing to expand coverage and/or local capability.

Key challenges identified being:

- Localisation and administrative requirements
- Coordination across global and local operations
- Lead times aligned to vehicle development cycles
- Workforce capability and training

The FCAI supports the Department in their work to address cyber security and software update risks. Successful adoption will depend on regulatory alignment with UN standards and provision of sufficient transition time, enabling industry to leverage existing global systems efficiently.

Additional comments

1. Strong support for full harmonisation with UN R155/R156.

2. Recognition and acceptance of existing certifications:

- A major priority is acceptance of existing UN approvals, including:
 - Certificates of Compliance (CoC) for CSMS and SUMS
 - UNECE type approvals
- Acceptance of management system certifications from recognised technical services.
- Stressing that:



- Re-certification or duplicate assessments in Australia would create unnecessary administrative burden
- Recognition mechanisms are essential for efficient and timely implementation

3. Need for sufficient lead time

- Adequate implementation timelines are critical and must be aligned with vehicle development cycles. A minimum 3 years for new models and 5 years for all models.
- Particularly considering:
 - Models developed for non-UN-regulated markets
 - Time required for:
 - System adaptation / development
 - Training and organisational readiness

James Tol

Technical Director

Level 1, 59 Wentworth Avenue, Kingston ACT 2604

+61 (0) 408 856 876

james.tol@fcai.com.au