HEAVY VEHICLE INDUSTRY AUSTRALIA

Cyber Security and Software Update requirements Submission

Heavy Vehicle Industry Australia

With over 300 members, represents and advances the interests of manufacturers and suppliers of heavy vehicles and their components, equipment and technology.

www.hvia.asn.au hvia@hvia.asn.au 07 3376 6266

Executive Summary

Consultation has begun around potential future adoption of current Cyber Security and Software Update Requirements, United Nations (UN) Regulation No. 155 and 156, in Australia. The Department of Infrastructure, Transport, Regional Development, Communications, Sports and the Arts have called for feedback from industry by May 2026.

If adopted in Australia, it is most likely they would be rolled into the Australian Design Rules (ADR's), given a unique ADR number and referenced within the new rules as is typical in Australia when adopting existing European regulation.

The consultation also sets out an alternative option for tackling cyber security and software in vehicles in utilising more generic and existing frameworks such as the Cyber Security Protection Act of 2024. However, adoption of the UN regulations is the departments preferred approach.

This submission collates the questions, experiences and feedback HVIA have received from members on this topic. It is understood by HVIA that there will be further consultation from the Department after this submission, and prior to any finalisation of futures ADRs for Cyber Security and Software Updates.

A high-level summary of member responses and concerns is listed below:

1. Many members support harmonising with United Nations Economic Commission for Europe legislation and in particular UN155 and 156. Many heavy vehicle suppliers in Australia already comply with these regulations because many vehicles are imported from Europe or other jurisdictions that adopt these standards.

2. UN155 and 156 do not address the risk of international (or local) OEMs behaving as 'bad actors'. If an OEM is to become a bad actor, these standards do not mitigate or protect from this. A bad actor, if motivated, can easily pass a strict audit. We are dealing with a very high technology and complex cyber environment. The Australian Government will need a different approach for this risk.

3. Not all brands of Heavy Vehicle in Australia can easily meet these standards. The effort to ensure compliance will take some years for these manufacturers to achieve. It is felt that 3 – 4 years notice on implementation of a new standard would be ideal.

4. HVIA request that the department provide a Regulatory Impact Statement to evaluate the cost of implementation of these regulations. In an industry where costs are ever increasing and rates appear to be going backwards; it is imperative to understand the cost implications of any new regulations.

5. Even for brands whose parent company and vehicles may meet the UN155 and 156 standards, it will still be a time and cost burden to ensure requirements are met locally and the correct administration, paperwork and oversight is administered.

6. For brands which do not inherit UN155 and 156 compliance, in particular Australian vehicle manufacturers and impacted local technology providers, some financial support should be made available to support this transition via the Future Made in Australia investment fund. Our sovereign capabilities form part of our National Cyber Security Strategy.

7. For Heavy Trailers, there is some work involved in ensuring that all brake suppliers have been adequately engaged, and equipment, training and licensing is obtained to meet the UN 156 requirements.

8. Concerns have been raised that the largest cost burden may be the external audit and certification process; rather than Original Equipment Manufacturer (OEM) solutions, equipment and licensing. Some estimates indicate external audit, and compliance certification could cost an OEM more than $500,000.

9. If OEMs were to be externally monitored or audited, the documentation required to satisfy an audit may account to a neat playbook and significant Intellectual Property, for a third party to use, to hack a given system.

1. Harmonisation with United Nations Economic Commission for Europe (UNECE)

Many members support harmonising with UNECE Regulations. Many heavy vehicle suppliers in Australia already comply with these Regulations because many vehicles are imported from Europe or other jurisdictions that adopt these standards.

We acknowledge that Cyber Security provisions selected for heavy vehicles (and any road vehicles) will fall under the overall Australian Cyber Security Strategy. The 2023 – 2030 Australian Cyber Security Strategy was released on 8 December 2022.

The strategy set out that Australia has high ambitions to be a world leader in Cyber Security by 2030[1] which requires the unified effort of government, industry and the community. *"Together, we can equip our community to reduce the impact of cyber incidents through improved cyber hygiene and clear advice on how to respond confidently when they occur."* said Hon Claire O'Neil MP. The vision is that by 2030, *"Australia is a trusted and influential global cyber leader, working in partnership with our neighbours to lift cyber security and build a cyber resilient region."*

With respect to harmonisation, it is likely that this will mean adopting some common Regulations and identified best practices relating to cyber security such as the proposed adoption of UN 155 and 156. The vision in the strategy also included that *"we have a sovereign and assured capability to counter*

[1] https://www.homeaffairs.gov.au/reports-and-pubs/files/2023-2030_australian_cyber_security_strategy_discussion_paper.pdf

cyber threats". This could infer that blind harmonisation with global standards is not possible or enough, as local considerations will be needed to combat offshore threats.

UN 155 and UN 156, which were first adopted in June 2020, were developed under the GRVA Working Group for Automated/Autonomous and Connected Vehicle (based on the tradition of using an acronym from the French *"groupe des rapporteurs*" and in this case responsible for "*véhicules automatisés"*). The GRVA is chaired by Germany, with Vice Chairs from China, Japan and the USA. Hence it is understood the UN Regulations from GRVA are not just 'European'; but additionally informed by most key global participants.

HVIA members were consulted around the proposal to adopt UN155 and UN156 regulations as localised ADRs.

Member Feedback:

1.1 Heavy Vehicles: Some heavy vehicle suppliers confirmed they have already adopted UN 155 and 156 in the vehicles they are importing.

1.2 Heavy Vehicles: All truck manufacturers who were consulted agreed that adopting UN155 and UN156 is inevitable. The UN standards are the only global ones which are clear on the auditing process and requirements, so it seemed logical that they have been selected as best practice to adopt in Australia.

1.3 Heavy Vehicle Provider: Manufacturers of non-European brands noted they cannot implement the UN regulations immediately. We recommend the Department consult directly with manufacturers/suppliers representing non-European brands to understand their unique challenges before finalising timing and requirements for cyber security and software updates. It was noted that work for UN 155 and 156 started in Europe around 2020 and will only come into force on July 1, 2026. This is 6 years for manufacturers to be prepared.

As such, 3 – 4 years is thought to be a reasonable time frame for Australian manufacturers or vehicle brands not intrinsically meeting UN155 and 156 to comply.

1.4 Heavy Vehicle Provider: We are already in the harmonisation pathway, Australia must comply. As an example, for one manufacturer with two brands, one brand works as it is European, the Second brand will need a separate plan as it is not European.

1.5 Heavy Vehicle Provider: It is very complicated to divide the operation and responsibility of the CS/SU Cyber Security/Software Update system between Parent company and local company which may be registered as a Second Stage Manufacturer (SSM). Additionally, it is difficult to manage the systems while considering all the equipment which may be fitted on the rear body by the second stage manufacturer and additionally disclosing of information to the SSM whilst ensuring CS/SU protections are maintained. This concern will be relevant for incomplete vehicles which are imported to Australia.

1.6 Heavy Vehicle Provider: Regarding the *Cyber Security Act 2024* – vs RVSA. We would rather 155 and 156 as ADRs. CSA is for mobile devices and not appropriate. We have concerns around industry applying multiple regulations for Motor vehicles generally.

1.7 Telematics Provider: Some members were concerned that the department has assumed that UN 155 and 156 should be exclusively adopted without consideration of other alternative and aligned standards. UN 155 and UN156 are just two of many cyber related international standards. Some others being followed are:

ISO SAE 201434 Cyber Security Best Practice

ISO 24089. Jap UNECE WP.29 Alignment

The concern was that a prescriptive focus on one standard may not reflect the bespoke nature of Australia with vehicles from multiple regions. There are cost concerns that the UN Regulations may not reflect processes which have already been adopted. If compliance with UN155 and 156 can be delayed 3 – 4 years, manufacturers could in the interim declare which standards they do meet for cyber security and software update, as almost all of them are currently meeting a somewhat equivalent local or international standard.
The department could conduct an audit through ROVER in the meantime of all OEM vehicle providers to understand what standards are being met.

1.8 Telematics Provider: How the auditing process would be managed in Australia is not clear. The vehicles from overseas are audited and validated in Europe. If they are imported to be sold in Australia, it is presumed that ADR compliance to Cyber Security will need to be declared via the ROVER platform and evidence provided. Will the UN evidence be sufficient for these vehicles as is typical for other ADRs based on UNECE? Or will there be localised requirements?

1.9 Telematics Provider: The ADRs are not perfect, but we want to reduce duplication. Being able to audit is already being managed well in other areas and many already comply. ADRs are sometimes seen as higher authority. We want to try to align, so there are no additional costs and processes.

1.10 All members: Will Australia employ an additional auditing process to check? For vehicles made in Australia or without a prior UN approval, additional cost will likely be incurred by these OEMs to generate a localised approval. The auditing process must be approached with caution as we do not want local OEMs to inadvertently create a manual on how to hack a device.

1.11 All members: UN155 and 156 do not address the risk of international (or local) OEMs behaving as 'bad actors'. If an OEM is to become a bad actor, these standards do not mitigate or protect from this. No level of auditing would prevent this either as the complexity of technology is too high. Industry encourages the Australian Government to be aware plan and reduce the likely consequences, of such a scenario. This may include provisions around where

the data is stored and managed (ie. onshore only), how OEMs are vetted, preventing OEM monopolies, Killswitch provisions, defence technology etc.

1.12 Fleet feedback: One operator reported near-daily issues with its electric truck fleet due to frequent over-the-air software and firmware updates. In some cases, these updates make chargers incompatible with the trucks, disrupting critical operations. Implementing UN156 would help by making software updates more transparent and easier to trace when bugs occur.

Consultation Questions:

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?
- 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?

Answers:

- Some OEM'S have already adopted UN155 and UN156.
- Working these regulations into Australian practices is still a work in progress as the regulations are only in full force in Europe from July 1, 2026.
- Some OEMs will not adopt UN155 and UN156 in Australia until it is mandated as there is significant cost and administration involved. This is even OEMs whose parent company is practicing UN155 and UN156. These OEMs are currently practicing cyber security and software update hygiene in their practices, just not reporting out to the standard until it is mandatory.
- OEMs are currently utilising best IT practice for cyber security management in their businesses and vehicles. OEMs utilise their own proprietary software for maintenance and software changes.
- Some telematics providers have used ISO SAE 201434 Cyber Security Best Practice and ISO 24089. Jap UNECE WP.29 Alignment

2. Implementation of Management Systems

Industry is well versed in meeting new ADR requirements relating to updated technology and testing. Hygienic Cyber Security and Software Management is a necessary requirement, but it will take some time and resource for OEMS to implement their management systems robustly.

Technology is moving at a rapid pace, faster than ever seen before by the road vehicle industry. There are many new regulations being introduced around emissions, driver assistance systems, vehicle safety requirements, tyre pressure management, on board mass, regulatory telematics, the move to zero emissions vehicles and autonomous vehicles just to name a few.

OEMs have teams of engineers and managers set up to handle the ever-changing technology and development environment. Competition to build these high technology vehicles quicker, cheaper and more efficient continues to accelerate.

As a result, New models must consider power management as a critical design feature. The more complex the ECU units and computer systems have the capacity to reduce the number of components as double ups in sensors, GPS units and valving for example. Previously stand-alone operating systems must now be integrated to reduce waste and improve maintenance and installation. Packaging, safety, materials, availability of critical components, Material safety data sheet requirements, the list of things to manage goes on.

It is fair to say, that with all this happening, the modern OEM is quite busy and must become a master in managing the many different requirements to meet regulations, remain profitable and still produce a desirable market competitive offering.

Cyber Security and Software Management systems add to this list. The OEMs accept that this is a necessary and imminent task, but they do need time to prepare with all their other critical and imminent tasks.

Members had the following feedback:

2.1 Heavy Vehicle Provider: It not so simple to say North American trucks alone are affected, we have many hybrids Part EU/Part NA. On this there are already so many demands for changes, not just cyber, But also Euro VI, EV's etc. There may not be enough resources to meet a short time frame. We've had recent poor experience with ADRs implemented in a short time frame and don't want to see a repeat. 3-4 years may be more realistic than 1 -2.

2.2 Heavy Vehicle Provider: Having a 'New models go first framework' as if typical with ADRs might not be appropriate, new models have been in design now for years. 2 years for these would still be too soon. In Europe when they released the new models go first for UN155 and 156, this led many OEMs to simply cancel new models for 2 years as they could not meet the time frame.

2.3 Heavy Trailer Provider: ECE 156 is the SUMS standard (Software Update Management System) which is driving factor as OEMs become accountable for their updates. ZF/Halder/Knorr/Schmitz have rigorous processes, to meet validation requirements. If SUMS is implemented in Australia the Electric Vehicle Truck example of surprise updates to software resulting in temporary charging incompatibility in point 1.12, should not be possible.

2.4 Heavy Trailer Provider: SUMs includes Fail-safe of standard, this means if there is an error in update, roll back protocol must be met.

2.5 Heavy Trailer Provider: It took 18 months - 2years for the counterparts in Europe to roll out SUMs for trailers. Some SUMS systems are not compatible with each other, so a trailer builder may need to buy 3 separate systems. Over past few weeks, we have been struggling to get information from suppliers despite EU counterparts.

2.6 Trailer EBS Provider: Regarding parameter updates in service. Currently, braking files are written by some distributers and not OEMs. It will be interesting to see how SUMS effects this. In the Aftermarket, Software of Trailer EBS systems is modified in service by non-OEM Aftermarket Tools and this sometimes includes changing of braking parameters which should only be modified by the OEM (or direct agent for the OEM).

2.7 Trailer EBS Provider: OEMs have raised concerns regarding the use of third-party diagnostic tools and parameters being changed by workshops. UN156 should address this scenario.

2.8 Fleet: A major fleet experienced 2 cyber security incidents a few years ago with great negative impact experienced. This drove higher reliance on local support vs Overseas support. Business cyber security is currently more of an issue than trucks themselves.

2.9 Telematics Provider: Many Heavy Vehicles do have over air updates now. For Cyber Security threat, online risk is rampant for all organisations. We have seen dramatic increases in proof of compliance. On site auditing of compliance from OEMs is at high cost in resource. Engineers doing assessments. Multiple audits. Standard questions – where your data is hosted, where does it travel, encryption including long term storage? With geopolitical climate, offshore data is higher concern. OIAC papers were broadly distributed today. Many questions raised such as '*Can I hack and disable thermal management systems for a battery?*' '*Is the Video camera imagery offshore?*'. Etc

Consultation Questions:

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?
- 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?

Answers:

- OEMs are not generally concerned about their internal capabilities or staff to meet the cyber security requirements. It is more of a time, planning and cost concern.
- There is some reliance on overseas staff as expected as the regulations are European.
- Many HVIA members have reported confidentially cyber incidences relating to their businesses and business systems (not typically vehicles). We are also aware of other businesses who have been hacked through employee laptops using phishing techniques to gain access to databases and requesting a ransom to retrieve the data taken or copied.
- Trailer EBS providers have raised concerns about third-party diagnostic tools being used to change parameters without OEM approval, which may compromise trailer ADR braking compliance. This is not seen as a malicious attack, but rather the result of poorly informed operators being given tools and access they are not qualified to use. It also raises questions about OEM liability, given they may remain responsible for a vehicle's cyber security for up to 10 years after the last unit is produced. If someone physically connects to a vehicle and uses a third-party tool to make an unauthorised change contrary to OEM guidance, it is unclear who would be liable. UN156 indicates that the OEM is liable, but it may not be so straight forward as this in practice as 'right to repair' legislation does mean third party tools will continue to access OEM systems.
- Regarding diagnostic interfaces, our understanding is that UN155 and 156 covers this topic thoroughly and there are processes in place where third party tools cannot be 'black boxes' and must log and report changes back to the OEMs. There is a delicate balance to ensure there is not a conflict with the 'Right to Repair' legislation. We understand this is covered by the UN Regulations and is being implemented in Europe. We should stay close to Europe to understand after July 1, 2026 when Regulations effect all vehicles, if this creates any issues for the aftermarket sector. Having a lag in our own regulations to Europe for this reason is beneficial in the interim.

3. Local impact to vehicles and control units

The impact locally is varied in Australia due to a mixed market of global and local technology products being supplied from all around the globe.

Australia is considered a mixed market when it comes to road vehicles. In contrast to Europe, where only trucks and cars meeting European standards are permitted to operate. Australia has imported vehicles from many countries including North America, China and Japan. This creates some differences in how vehicles within the Australian market operate and what regulations they comply with.

Typically, all heavy vehicles will comply with UNECE or local ADR regulations. The ADRs set out multiple clauses for compliance which deviate from the UNECE, which results in imported vehicles either being modified once they arrive in Australia or being built in Australia to slightly different specifications than their international counterparts. Common examples are:

- Australia's vehicle and trailer width requirements of 2.5m. It was only recently that wider trucks were allowed to 2.55m which is equivalent to the European requirements, but only if meeting the Safer Freight Vehicle parameters.

- Trailers must be parked '*via mechanical means*'. The result of this localised requirement is that every imported truck which can tow a heavy trailer must be modified to ensure that the supply line is exhausted by the park brake so that the trailer spring brakes are engaged under parking.

- In Australia the driver sits on the right side of the vehicle, which results in a physically different packaging and location of componentry. This is contrary to both Europe and North America, and puts us in the same category as approximately 35% of the world including the UK, Japan, India and South Africa.

The impact this has on any ADR adoption of UNECE regulations, is that there will always be some local considerations. In the case of cyber security, the main consideration is which nations have adopted or will soon adopt UN155 and 156, and how the Regulations will be drafted and applied in Australia.

According to a United Nations Press Release in 2021, Japan was one of 54 countries who adopted both UN Regulation 155 and 156. North America has not yet adopted the regulations, however, some manufacturers within North America may voluntarily comply with the globally developed UN standards. China has its own localised National standard known as GB 44495-2024.

Members had the following feedback:

3.1 The main concern from all members is that the Australian government understands that for local suppliers whose parent companies are not from Europe or Japan, these standards pose an increased challenge, time impetus and cost. Even for suppliers who are of a European base such as the Trailer EBS providers, there are local challenges in the roll out of upgraded diagnostic equipment and proprietary software. Workshops and fleets will incur additional costs moving forward to have access to diagnostic equipment and additional training is required for diagnostic users.

Consultation Questions:

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?

- Many Heavy Vehicles sold in Australia are European. In 2025 ≈36.5% of new heavy trucks sold were European, ≈31.3% were North American and 32.1% were Japanese. The Japanese vehicles are likely to adopt UN155 and 156 in the future. North American vehicles may not, hence generating a localised requirement for 31.3% of vehicles to 'manually' comply rather than inheriting compliance from a parent company. Chinese commercial vehicles are becoming more common in the Australian marketplace, but in the heavy space make up less than 1% of sales.

- Due to the 2019 mandate for Trailer EBS to be fitted to most trailers in Australia, ≈90% or more of trailer control system CTAs are likely to be impacted by the UN 156 SUMs requirements. A small proportion of trailer braking systems which are not mandated to use Antilock and Vehicle Stability technology will not be affected. Currently there are three Trailer EBS manufacturers on the Australian market. All three manufacturers are European based and hence have a UN156 compliant SUMs system being deployed in Europe currently.

- Telematics, tyre pressure monitoring, on board mass and other auxiliary suppliers may get caught out by these requirements. Many units are either locally developed or, Chinese, North American based and will need to invest locally to meet the proposed requirements. Relevant CTAs, if in place for new builds, will be affected.

- It is unclear what effect these new mandates have on VSB 6 and Heavy Vehicle Modification or aftermarket fitment of telematics or auxiliary systems with electronic control units. This will need to be considered upfront in the roll out of any new ADR and not as an afterthought.

4. Biggest Adoption Challenges

Members highlighted the largest challenges or concerns being the time frame given to meet the new proposed requirements and the potential for unnecessary red tape and cost to be introduced in the auditing or compliance process to be chosen locally.

When new ADRs are introduced and based on European standards, the ROVER system which receives compliance information for new vehicles and subsystems, is well equipped to receive applications. These applications are checked and processed within 30 – 60 days. Applicants are audited by the department via desktop or in person at semi-regular intervals.

Audits are only ever at the systems levels. It is very rare for the department to inspect test reports or results in detail as it is understood to be the OEMs legal responsibility to comply with the ADRs. OEMs accept when they apply, that failure to comply, could result in legal liability if a critical incident is due to nonconformity.

Industry has interpreted the UN155 and 156 regulations, to assume the same general process and principles. Manufacturers must submit test or evidence reports which demonstrate compliance with the regulations and the onus is on the manufacturer to ensure that they maintain compliance and support their product throughout its life and in the case of UN155, for 10 years after a vehicle type completely ceases production.

If this is the level of compliance to continue under the new standards, the increase in administration and technical work for OEMs is considered fair and reasonable if appropriate time and notice is given to comply.

If there is to be an external audit process implemented, there would be some concerns by industry in firstly having auditors with the right level of technical knowledge and qualification to audit a vehicle's cyber security robustness. Additionally, the cost of such a process would need to be reasonable.

Members had the following feedback:

4.1 Heavy Truck Provider: UN155 and 156 allows a means to demonstrate compliance before something has happened. There would have to be an Australia Government auditing process if we were to implement other international standards.

4.2 All: A key concern is that EU legislation applies for the life of the vehicle, making the OEM responsible throughout that period, whereas ADR obligations generally apply only up to the point of sale. If a third party alters OEM files after gaining physical access to the vehicle with permission from the operator, it is unclear how the OEM could remain responsible. Telematics may help identify changes, but restoring the system may not be possible if it has been physically tampered with.

4.3 Telematics Provider: The government is currently looking at device labelling. Software firmware processes are being audited. The instruction was to hand over firmware for testing.

No-one is comfortable doing this as it is a playbook on hacking. Prescriptive approach is of concern, threat vectors etc.

4.4 Telematics provider: For ISO 27001- Already external cost levels are enormous, ie $500k + $50k chunks from assessment to audit. Global best practice required to avoid cost blow out. We do not want to see this level of cost introduced to industry to implement these regulations.

4.5 Telematics provider: There are limited local cyber security compliance assessors, so, the industry may need to rely on international auditors, which could lead to a capability gap.

4.6 Trailer Builder: Auditing would operate based on checking that there is a system in place. Would the Department, NHVR and/or a third party be used for this task?

4.7 Trailer EBS provider: We don't believe that Australia has the resources for your Option 2. If we did create something with unique features, it would be unrealistic for suppliers to modify their software to our standard particularly if they already comply to an existing world standard

Consultation Questions:

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?
- Any additional comments?

- The two biggest concerns provided by members were:
    - Time, resource and cost to meet these requirements and needing a lot of notice to plan this task and ensure the right expertise. For brands which do not inherit UN155 and 156 compliance, and particular Australian vehicle manufacturers and impacted local innovators and technology providers, some financial support should be made available to support this transition via the Future Made in Australia investment fund. Our sovereign capabilities form part of our National Cyber Security Strategy.

    - Concerns that localised auditing may be implemented and increase external cost and red tape. It was noted by members that concerns around OEMs becoming 'bad actors' is not covered in these regulations. **The Australian Government will need a different approach for that risk** which is unlikely to be effective if it is a strict audit of UN155 and 156. **A bad actor, if motivated, can easily pass a strict audit**. We are dealing with a very high technology and complex cyber environment.

5. Questions for the Department

Points for clarification

5.1 Can you confirm if auditing would only operate based on checking that there is a system in place? If so, would the Department, NHVR and/or a third party be used for this task? Will there be a cost to industry for this audit?

5.2 Can you indicate a time frame you are considering for adoption of these regulations into ADRs?

5.3 Will the rollout be 'classic', ie. OEMs simply submit their evidence into ROVER and CTAs relating to these ADR requirements? Or will there be special and/or localised measures included? Has the SSM process adequately been considered in the proposed rollout of new regulations?

5.4 Will either the 'Future Made in Australia' funding or an equivalent sovereign funding source be made available to assist local vehicle manufacturers and technology innovation providers with the adaptation of UN155 and UN156?

5.5 Can a Regulatory Impact Statement be provided for the proposed introduction of new regulations for Cyber Security and Software Update?

Conclusion

This is just our first formal response regarding consultation on the proposed adoption of Cyber Security and Software Update regulations UN 155 and UN 156. It is our understanding that further consultation will continue prior to the release of any ADRs on this topic. We will require adequate time to review the draft ADRs with our members and ensure that all relevant requirements, concerns and challenges have been considered prior to implementation. There is a big task ahead to educate industry around these new requirements and additionally outside of vehicles, on other cyber security requirements which will affect all businesses moving forward.

We do have concerns that localised auditing may be implemented and increase external cost and red tape. It was noted by members that concerns around OEMs becoming 'bad actors' is not covered in these regulations. The Australian Government will need a different approach for that risk which is unlikely to be effective if it is a strict audit of UN155 and 156. A bad actor, if motivated, can easily pass a strict audit. We are dealing with a very high technology and complex cyber environment.

Industry will need forward notice and time to ensure that all requirements are met without delaying vehicle production or release to market. Industry was very firm that 2 years would be too short a time frame, that Europe essentially had 5 – 6 years and hence 3 – 4 years may be a sensible compromise.

For further information, please contact Heavy Vehicle Industry Australia.