Australian Telecommunications Alliance

Setting The Standard.
Driving Progress.

AUSTRALIAN TELECOMMUNICATIONS ALLIANCE SUBMISSION

To: Department of Home Affairs

Re: Streamlining and Modernising the *Security of Critical Infrastructure Act 2018*

7 August 2026

CONTENTS

1. AUSTRALIAN TELECOMMUNICATIONS ALLIANCE

1.1 The Australian Telecommunications Alliance (ATA) is the peak body of the Australian telecommunications industry. We are the trusted voice at the intersection of industry, government, regulators, and consumers. Through collaboration and leadership, we shape initiatives that grow the Australian telecommunications industry, enhance connectivity for all Australians, and foster the highest standards of business behaviour. For more details, visit www.austelco.org.au.

1.2 For questions on this submission, please contact Deputy CEO Christiane Gillespie-Jones, c.gillespiejones@austelco.org.au.

2. INTRODUCTION

2.1 The ATA welcomes the opportunity to provide a submission to the Department of Home Affairs (Department) in response to its Consultation "Paper Streamlining and Modernising the *Security of Critical Infrastructure Act 2018"* (Consultation Paper). We commend the Department for the development of a clearly structured and well-articulated Consultation Paper.

2.2 ATA members are acutely aware of the role that their networks, infrastructure, and services play in the Australian economy and for the cohesion of Australia's society. Accordingly, they take security very seriously and continue to make substantial, ongoing investments into further enhancing the resilience of their networks, infrastructure, and systems against cyber attacks, natural disasters, and other hazards.

2.3 We focus our submission on the proposed measures and their respective key design elements as they relate to the telecommunications sector rather than responding to the 121 individual questions of the Consultation Paper.

2.4 ATA members may make individual submissions, including on issues that may relate to other critical infrastructure sectors.

2.5 We stand ready to further engage with the Department and other relevant stakeholders on the streamlining and modernisation of Australia's national security legislation, to ensure that all aspects of critical infrastructure legislation harmonise within our sector and, where appropriate, also across sectors which share significant interdependencies with our sector, e.g. the energy and data storage and processing sectors.

3. OVERARCHING COMMENTS

3.1 We support the Government's intent to continually streamline and modernise security legislation for critical infrastructure, including through the removal of complexity and duplication from *the Security of Critical Infrastructure Act 2018* (Act).

3.2 We also welcome the commitment to further consult on potential changes to rules and subordinate regulation. To ensure any additional or amended regulation is proportionate and practical, consultation ought to be sector-specific, comprehensive, not unduly time-constrained, and be undertaken through a true co-design process between Government and our sector. The approach taken for the development of the telecommunications sector rules through the Australian Telecommunications Security Reference Group (ATSRG) may serve as a reference for a pragmatic and effective co-design process.

DEFINITIONAL CONCERNS

3.3 We are conscious that the proposed reforms follow the independent review of the operation of the Act by Dr Jill Slay AM in late 2025/early 2026. Unfortunately, it appears that key definitional issues are not being addressed by the proposed reforms. We reiterate our concerns in this regard.

3.4 The definition of 'critical telecommunications asset' in section 5 of the Act remains excessively broad due to the inclusion of the defined term 'asset', which extends to a system, network, facility, computer, computer program, computer data, premises and any other thing [emphasis added]. While guidance materials have proven helpful, the existing definition does not provide sufficient certainty to responsible entities about excluded assets, and this certainty is necessary for responsible entities to understand their own obligations under the Act as well as the obligations of other entities in their supply chains. We suggest the definition of critical telecommunications assets be amended to remove this uncertainty and more intentionally capture the infrastructure, systems, and services that are critical to the availability, integrity, or confidentiality of telecommunications within Australia.

3.5 Similarly, the definition of 'data storage systems' has a very wide scope which muddies what is in fact critical to operations. The definition captures systems that 'process' business critical data. There is no definition given for 'process' so we assume this includes transporting data from point A to point B, regardless of whether there is any transformative effect on the data. Applying this definition of 'process' means most systems in a telecommunications provider technology stack are in scope, and entities cannot focus on their crown jewel systems. We consider this can have the unintended effect of entities losing focus on what systems are truly critical to operations. A clarification would also be relevant as telecommunications providers may store business critical data in site locations rather than data centres.

3.6 The framework applies without regard to the scale or significance of the entity involved. It imposes obligations on entities that are not critical infrastructure in truth and reality. Every carrier is captured by reason of its licence alone, and a CSP is captured wherever its asset is used in connection with carriage services supplied to a Commonwealth entity, however limited or peripheral that supply may be. Small CSPs rarely have dedicated security, legal, or compliance functions, the fixed costs of compliance fall on a very small revenue base, and the obligations must be met from the same limited technical resources that operate the network. We suggest that the Rules include an express critical infrastructure threshold, adding to the criterion already used in section 51(1)(c) of the Act. The threshold should have regard to matters such as the number of end-users and the geographic area that would be affected by the compromise or unavailability of the asset, whether the services supplied to a Commonwealth entity support a critical function of that entity as distinct from administrative, incidental, or readily substitutable supply, the availability of substitutes, and any interdependency with other critical infrastructure assets. Such a test would ensure that the compliance effort of industry and the supervisory effort of the Department are concentrated where they deliver a genuine security dividend and would complement the exemptions framework proposed under Measure 1 by answering the anterior question of whether an asset warrants regulation under the Act at all.

3.7 As the regime develops past its infancy into a more mature and better understood framework, it would be good to get clarity (ideally through guidance) as to common understandings between Government and industry.

3.8 For instance, we remain concerned that there may still be uncertainty about what level of granularity should be adopted in identifying critical components, and this affects the level at which controls may be adopted. As the CISC and the Department receive information from each critical infrastructure sector, we think it would be beneficial for it to share, through industry guidance, its preferred (or at least the most common) levels of granularity which are applied.

3.9 Further guidance would support industry's understanding of threshold questions such as those relating to the 'materiality' of risks and the threshold for a 'relevant impact' on an asset that would be reportable as a mandatory 'other' cyber incident. Taken generally, we appreciate that Government is concerned with the sort

of risk that affects large numbers of people, large areas of geography or otherwise may significantly and adversely impact the economy or national security. However, this broad understanding exists alongside (and in many cases incongruently with) industry-specific regulatory frameworks that set thresholds for various sector-specific regulatory interventions (e.g., the recent telecommunication regulations applicable to network outages and Triple Zero calls) on the basis of some version of a 'significance' or 'materiality' test. We take the view that, where possible, guidance should be given about whether those industry specific thresholds should be taken as de facto indicia of 'materiality' or whether it is intended to apply some other threshold or degree.

3.10 It would also be helpful to see guidance on the interaction of the requirements around 'protected information' with the information sharing requirements contained on other regulatory instruments, e.g., the *Telecommunications (Customer Communications for Outages) Industry Standard 2024* and the *Emergency Call Services Determination 2019*.

3.11 We also note that the definition for a 'cyber security incident' in the Act does not align with the *Guidelines for Cyber Security Incidents* published by the ASD's ACSC. It would be helpful for industry if there were alignment on this definition.

3.12 In relation to the hazard areas, there is overlap between the definition of physical security hazards and natural hazards. Further guidance as to how these two hazard areas can be distinguished would be helpful.

REGULATORY IMPACT

3.13 The Consultation Paper considers each reform and assesses the regulatory burden for each proposed measure individually.

3.14 However, in practice, these reforms do not operate in isolation and, consequently, ought to be assessed for their regulatory impact jointly. Responsible entities will need to comply, for example, with new requirements relating to supply chain cyber assurance, relevant operator arrangements, corporate group cooperation, independent CIRMP assurance, and the expanded critical worker framework. Many of these obligations extend to suppliers, operators, and related entities, requiring organisations to identify, assess, and manage these relationships, including through contractual arrangements. As a result, the overall compliance burden – particularly for entities with complex outsourcing models or concentrated supply chains, such as telecommunications carriers – is likely to be significantly greater than the sum of the impacts of each single reform considered in isolation.

4. MEASURE 1 – EXEMPTIONS FRAMEWORK

4.1 We support an exemptions framework where another Commonwealth, State or Territory law, or another recognised enforceable framework, delivers substantially equivalent or stronger outcomes.

4.2 In order to maximise the benefits from the proposed exemptions framework, we recommend that it:

a) allow obligation-specific exemptions;
b) include clear decision criteria;
c) provide transparent timeframes for decision-making;
d) support regulator-to-regulator coordination; and
e) avoid requiring multiple audits against substantially similar controls.

4.3 The telecommunications sector is subject to a raft of regulations that contain aspects that either directly or indirectly relate to the requirements of the Act. We believe some of these existing regulations ought to be

considered forming the basis of an exemptions framework for the sector.

4.4 However, while we are supportive of an exemptions framework and consider that some of the existing regulations ought to be assessed for their suitability for equivalence, we highlight the need to ensure that additional obligations that are duplicative or, worse, inconsistent with the requirements of the Act are not being introduced into (non-SoCI) telecommunications sector-specific legislation and regulation. We observe a tendency that such regulation, for example in relation to scam prevention, seeks to introduce requirements in relation to the security of networks where equivalent requirements already apply in the SoCI Act. This introduces unnecessary compliance complexity and regulatory burden for our sector. Therefore, it would be helpful to clearly 'designate' the Act as the primary source of requirements for the security of critical telecommunications assets and require other Government departments and regulators to consult with the Department on any measures that they wish to introduce into telecommunications (non-SoCI) regulation, to ensure the already existing myriad of regulations that entities are required to comply with for the security of networks does not further increase or diverge.

5. MEASURE 2 – REGISTER OF CRITICAL INFRASTRUCTURE ASSETS

5.1 We support the proposal in principle and welcome the focus on key system and suppliers and more specific guidance on asset registration form and a format that is asset class-specific

5.2 We submit that the information to be provided ought not to increase from current levels or duplicate other SOCI reporting requirements.

5.3 We are concerned that the proposed notification trigger (awareness) may result in a constant stream of updates. It appears to be more practical to require periodic notification to allow regulated entities to batch notifications.

5.4 We look forward to consultation with our sector on the detail of registrable information.

6. MEASURE 3 – CIRMP ANNUAL REPORTING SIMPLIFICATION

6.1 In principle, members are agreeable with the proposal to give an annual compliance report in a prescribed form.

6.2 However, members are also concerned that significant variation in the questions for response may limit the 'repeatability' of reporting and, associated with this, the opportunities for the reporting to grow in maturity and value over time.

6.3 Consideration ought to be given to maintaining the current approach with an additional option for reply on specific questions. Alternatively, the prescribed form could contain a standard core set of questions with only a limited number of additional, annually varying questions.

6.4 We note that in all circumstances, it is critical that the prescribed form (and associated questions) be made available to responsible entities with a six months' lead time. In any case, we believe that the information that can be requested ought to be limited to information that the responsible entity can provide without modification or development of new systems that would be needed to produce that information.

6.5 Consolidated corporate group reporting ought to be available for responsible entities but not be mandated as consolidated reporting may not be useful or viable for telecommunications providers that are functionally separated, do not have a shared asset base, or where the distinctly owned asset bases are regulated differently under the Act.

7. MEASURE 4 – PART 2D NOTIFICATION CLARIFICATION

7.1 It is unclear what the proposed reform will achieve beyond the creation of additional legal certainty for the Department and whether there have been any issues in the past that would be addressed through the additional clarity that the proposal expects to provide.

7.2 In any case, our members believe that clear guidance on the (re-)notification threshold ought to be provided to responsible entities, including through case studies. Consideration could also be given to providing case-specific guidance as to what types of changes the Department would expect to be notifiable at the time when initial approval is being granted.

7.3 For example, re-notification may be warranted where the notification threshold is met because a new material risk is identified or where key risk assessment information in the previous notification becomes inaccurate or outdated. By contrast, changes such as revised project timelines, implementation sequencing, or minor variations to controls that achieve an equivalent risk outcome should not, in our view, require re-notification.

7.4 Equally, we believe additional clarity is required as to when a new service would require notification. For example, a new service using new assets may require notification, whereas a new service using an existing asset base would, in our view, not be notifiable.

7.5 We query the need for increased civil penalties to emphasise the need for timely notification. Has the Department observed a significant number of late notifications that would warrant such increases? If the Department has identified compliance concerns within specific parts of the sector, a more targeted compliance and enforcement approach would be preferable to a blanket increase in penalties across all regulated entities.

8. MEASURE 5 – CYBER SECURITY INCIDENT DEFINITION: AUTOMATED SYSTEMS, SOFTWARE AGENTS AND AI

8.1 It should be noted that on a level of principle, an incident triggered by automated systems, software agents or AI, is not necessarily different from other types of incidents, including those resulting from automation, given any reportable incident must meet the materiality threshold test. Equally, threat management systems and processes are also unlikely to differentiate on whether automated action was introduced and executed via script, a comprehensive frontier model, nation-state threat actor, or an insider.

8.2 However, we support clarifying the definition of a cyber security incident to ensure that incidents involving automated systems, software agents and artificial intelligence are properly encompassed. Any amendment should, however, remain technology-neutral and avoid unintentionally deterring the legitimate use of automation for cyber security, network management, or operational resilience.

8.3 Having clarity of definition is relevant for telecommunications services as they increasingly rely on software-defined networking, automated configuration, and monitoring, while data management makes growing use of automated control, environmental monitoring, and facilities management systems. In particular, for telecommunications networks, as network infrastructure and systems technology advances towards 6G and AI-native infrastructure, there will be increased adoption of AI based features to support network optimisation, performance, and fault diagnosis. This technology should not, of itself, be seen as creating increased cyber security risk. Broad inclusion of AI in the definition of a cyber security incident should be considered through this lens and in particular with respect to the applicable test.

8.4 Therefore, we recommend that the applicable test focus on whether an automated system, software agent, or artificial intelligence capability materially compromises, or has the potential materially to compromise, the availability, integrity, reliability, or confidentiality of a critical infrastructure asset or system. The mere use of automation should not, of itself, be regarded as presenting a risk. In this context, the ASD's and Department's advisories (including to Government and in relation to the PSPF) may also provide guidance on definitions and risks associated with systems, software agents, and AI.

8.5 This approach would advance the Consultation Paper's objective of strengthening agility in responding to emerging threats, while avoiding unnecessary regulatory uncertainty for legitimate defensive and operational uses of automation.

9. MEASURE 6 – SYSTEMS OF NATIONAL SIGNIFICANCE

9.1 The proposed shift from cyber incident response planning to broader resilience planning is likely to require significant uplift in preparedness, continuity and recovery planning obligations. This may involve development of asset-specific resilience plans, additional governance processes, exercises, playbooks and staff training. The potential impacts for telecommunications providers include:

a) Development of asset-specific resilience plans and recovery playbooks across all hazard types;
b) Expanded focus beyond cyber incidents to continuity, restoration and service recovery;
c) Additional governance, documentation and assurance requirements;
d) Increased training and awareness activities; and
e) Increased compliance and regulatory costs.

9.2 We support the recognition of equivalent arrangements where those exist to ensure SoNS are not burdened with additional overlapping requirements. We suggest the Department could vet and publish approved equivalence decisions so that other applicants benefit from work already undertaken, and resources within the Department are used efficiently. Effectively, this means that equivalence could be established for a class of responsible entities rather than each entity individually.

9.3 Noting the range of potential impacts, we submit that the proposed changes require an implementation period of at least twelve months.

10. MEASURE 7 – SUBMARINE TELECOMMUNICATIONS CABLES AND ASSOCIATED INFRASTRUCTURE

10.1 Regulatory obligations should remain focused on entities that own, operate or exercise effective control over submarine cable systems and associated infrastructure. Expanded asset coverage should be accompanied by clear sector-specific guidance, proportionate thresholds, and explicit exclusions for equipment suppliers and service providers that do not direct, manage, or control the operation of the asset. Any reforms should avoid inadvertently increasing compliance costs or limiting access to globally sourced technology and expertise. Responsibility under the SoCI framework should be allocated according to actual operational control and risk ownership, with asset owners and operators remaining accountable for compliance obligations, while passive investors, minority interest holders, and suppliers performing discrete technical or support functions are not captured as responsible entities.

11. MEASURE 9 – SPACE TECHNOLOGY

11.1 The feedback on this measure was provided by the members of the ATA Satellite Services Working Group (SSWG).

11.2 The Consultation Paper proposed four asset classes to give operative effect to the existing space technology sector: ground segment infrastructure, positioning, navigation and timing support infrastructure, earth observation data infrastructure, and space situational awareness infrastructure.

11.3 It proposes that the asset class 'ground segment infrastructure' cover *"terrestrial systems in Australia used for command, control, telemetry, tracking, uplink, downlink, data reception, mission operations, tasking, scheduling, network management or associated operational support for satellite systems."* The definition for the space technology sector in the SoCI Act, Note 1, includes 'communications' as one of the examples of space-related services, along with the other satellite system services mentioned in the proposed 'ground segment infrastructure' asset class. This could capture critical space technology assets which provide critical communications services but are not a carrier or a carriage service provider service nor provide a broadcasting service.

11.4 Taking into account the above conditions, one option that could be considered is to include 'end-user communications' in the SoCI Act for the proposed asset class 'ground segment infrastructure' but limit critical assets to those functional classes providing public safety, emergency, security, or critical defence services. If such a limiting criterion was applied to space technology 'end-user communications', then ground segment infrastructure could cover terrestrial systems in Australia used for command, control, telemetry, tracking, uplink and downlink end-user communications, data reception, mission operations, tasking, scheduling, network management or associated operational support for satellite systems. Examples would come from many industry sectors including aviation, maritime, finance and defence who operate closed satellite communication networks not connected to the PSTN or internet.

11.5 As highlighted above (under Measure 1), the ATA supports the policy objective of reducing duplication and simplifying the SOCI framework to ensure that relevant operators are clear on their obligations and can focus on uplifting security, rather than navigating overlapping and complicated configurations of regulations which aim to provide materially the same practical outcome.

11.6 We agree with the Department's observation that there may be critical infrastructure assets in the space sector that may meet the definition of both a space asset and a telecommunications asset (or an asset definition of another sector) and, consequently, requirements of two or more sectors could be applicable unless specifically excluded.

11.7 We strongly support the proposal that the risk of potential overlap and duplication is managed through a clear framework so that only one set of rules apply to assets that meet the definitions of both asset classes.

11.8 Accordingly, telecommunications sector RMP and other regulations ought to continue to apply to assets that are already being captured in the existing critical telecommunications asset definition.

11.9 We expect substantial consultation with the space sector will be required to develop clear asset classes and to delineate those from telecommunications asset classes.

12. MEASURE 15 – CIRMP GOVERNANCE AND ASSURANCE

12.1 We only support strengthening CIRMP governance and assurance arrangements where doing so produces demonstrable improvements in risk management. Assurance requirements should not, however, create an additional layer of duplicative, process-driven compliance.

12.2 Therefore, we recommend that CIRMP assurance be directed principally towards assessing whether relevant controls are effective in practice. The production of further documentation should not be treated as an end in itself, unless it materially contributes to improved security outcomes.

12.3 Moreover, the Department ought to recognise equivalent assurance evidence generated under other relevant security obligations and customer assurance frameworks. Enabling a single, coherent evidence base to satisfy multiple regulatory and assurance regimes would be directly consistent with the Consultation Paper's objective of reducing unnecessary duplication.

12.4 Against this background, we question the introduction of a requirement for independent auditing of CIRMPs. Due to the complexity of telecommunications networks and the significant, detailed expertise that is required, independent audits may not produce the expected benefit while increasing the risk that may be associated with the disclosure of information to third parties involved as a result of the independent auditing process, and introducing significant additional compliance costs for audited entities.

12.5 The proposal for independent audits is at odds with other regimes, such as the Hosting Certification Framework (HCF) which does not contain requirements for independent audits of CIRMPs. The HCF focuses on Government data and, therefore, ought to present a higher bar than the SoCI framework. Therefore, it is unclear why the SoCI framework intends to apply independent audit requirements for CIRMPs more broadly.

12.6 Moreover, we assume that many entities already work with independent advisors and external legal advice to develop their CIRMPs which, subsequently, must be approved by a responsible entity's board.

12.7 If independent auditing was indeed considered necessary, we recommend that the Department clarify the functions, requisite independence, and appropriate qualifications of assurance providers, and calibrate the frequency and intensity of assurance activities by reference to risk and materiality. Unlike other regulatory frameworks, the Act does not currently provide for a recognised auditor accreditation scheme or minimum competency requirements. Establishing minimum competency standards, or a recognised accreditation framework, would promote greater consistency in assurance outcomes and provide confidence that assessments are focused on the risks and controls most relevant to the SoCI regime. We also propose a broader consideration of the use of internal assurance functions. These consist of professional accredited auditors who are capable of providing independent verification.

12.8 We object to the proposal to remove current limitations so that annual compliance reports may be relied on in civil penalty proceedings. We consider the current admissibility restrictions are more likely to encourage a frank and open dialogue which benefits the broader security posture of critical infrastructure sectors.

12.9 Instead, we recommend that the Department provide clearer guidance on how entities can manage and mitigate enforcement risk when disclosing self-identified instances of non-compliance. Establishing a clear and transparent framework for voluntary disclosure would encourage continued self-reporting, support timely remediation of issues, and strike an appropriate balance between collaborative regulatory oversight and effective enforcement.

12.10 In addition, a removal of such limitations may also see compliance reports shared with third parties, such as law firms, thereby potentially diminishing the security of information provided. Moreover, responsible entities may not have visibility of such sharing arrangements.

12.11 In order to increase efficiencies, the Act could be amended so that, where the information contained in annual compliance reports is required in civil proceedings, responsible entities have the option to grant permission for the Department to release the information, subject to case-specific requirements with respect to transparency and security.

12.12 We support the proposal to strengthen CIRMP governance by requiring a minimum review cycle of 24 months with an approval of reviewed/updated/varied CIRMPs by senior management. If this review cycle is to be supplemented with additional events-based triggers, we recommend such triggers to be subject to sufficiently high thresholds to avoid responsible entities entering a cycle of review that, by virtue of a (low) threshold, results in frequent reviews where no materially changed risks are to be assessed and approved. Any event-based trigger ought to re-start the 24-month cycle.

13. MEASURE 16 – GRADUATED CIVIL PENALTY SETTINGS

13.1 We disagree with the proposal to increase penalties for core preventative and assurance duties.

13.2 As far as members are aware, the Department has not taken any formal enforcement action in relation to such matters, suggesting that the extent of non-compliance, if any, so far has not justified enforcement action. Accordingly, we seek evidence that an increase in penalties is indeed necessary to incentivise compliance.

14. MEASURE 17 – OPERATIONS AND MAINTENANCE AND MANAGED SERVICE PROVIDERS

14.1 Measure 17 proposes to introduce a new 'relevant operator' concept whereby entities that exercise material practical control over a critical infrastructure asset on which the asset materially depends may be classified as a relevant operator. Relevant operators would have duties imposed on them, including, a duty to cooperate, a duty to notify the responsible entity of material changes, and a duty not to take or omit action that would materially compromise a critical asset. The proposal would also require responsible entities to identify relevant operators and register them with Government.

14.2 Critical infrastructure providers, including telecommunications infrastructure providers, have complex supply chains often with hundreds of suppliers and those suppliers will often have their own sub-contracting arrangements. These supply chains may extend to overseas suppliers.

14.3 We recommend that the relevant operator concept be narrowly scoped, so as not to unnecessarily capture an overly broad range of entities. We support the position that the responsible entity under the SoCI Act remains the primary regulated entity but note that a relevant operator concept that is not sufficiently narrowed or clear could encourage an indirect 'offloading' of regulatory obligations from a responsible entity down the supply chain, in particular where the responsible entity largely decides whether a supplier is classified as a relevant operator. Consideration should be given to concepts and definitions that can logically translate from an operational perspective. Therefore, clarity of obligations and duties on certain suppliers is welcomed but must be balanced with what suppliers can reasonably be expected to manage operationally.

14.4 Importantly, any proposed reforms ought to include 'anti-overlap provisions' to clarify that an entity that is a relevant operator will not assume additional obligations or liability under the SoCI Act if it also has such obligations directly as a responsible entity in respect of the same assets.

14.5 Direct statutory obligations on service providers should also only apply where the provider has material practical control over the operation, availability, integrity or security of a critical infrastructure asset or critical function, and must only apply to that respective asset and/or function. A provider ought not become directly regulated merely because it supplies telecommunications, hosting, cloud, cyber security or support services to a SoCI-regulated customer.

14.6 It is also imperative that the reforms clarify that a provider does not exercise 'practical operational authority' merely because it supplies a service that is a material dependency for the operation of a critical infrastructure asset. In many cases, telecommunications providers may represent important dependencies for a critical infrastructure asset. However, a material dependency should not be confused with operational control.

14.7 Therefore, the legislation and any associated guidance ought to clearly define material practical control, clearly delineate operational control from service provision, clarify incident notification pathways and the interaction between contractual obligations and statutory duties, and provide safe harbours where providers

act on customer instructions.

14.8 The proposed reform envisages safe harbour provisions for responsible entities where effective cooperation arrangements with relevant operators cannot be achieved, subject to the responsible entity documenting the refusal, implementing a mitigation plan, and disclosing the gap in annual reporting. Given these substantial conditions and caveats, we seek clarity of the evidence which would be deemed acceptable, what mitigation would entail, and how the safe harbour provisions would work in practice.

14.9 Irrespective of these concerns, we highlight that imposing a registration obligation on suppliers because of their contractual relationship with an Australian SoCI regulated entity may deter investment and support for Australian businesses and increase concentration risk. The proposals are also likely to increase costs in supply arrangements for critical infrastructure providers as the additional effort and risks will be priced in by relevant suppliers. Commercial contracting may be unreasonably constrained by obligations under contract, that are duplicative of, or seek to go beyond, those already imposed as direct duties on a relevant operator under the Act. Unavoidable increases in regulatory and contractual risk may be priced in by relevant suppliers. In some instances, where increased risk cannot be priced in or otherwise reasonably managed by a supplier, it may be left with little choice but cease supply to the regulated entity.

14.10 Against this background, we query whether a registration approach is indeed necessary, or whether the APRA CPS 230 model, which only requires the regulated entities to report their material arrangements, could provide a more practical approach.

14.11 Alternatively, we recommend that the proposed reform remove the identification and registration step and simply make it a general duty for organisations who are critical infrastructure 'supply chain elements' to 'consolidate, coordinate, and cooperate' with responsible entities on hazards. The drafting could look similar to the duty under section 46 of the *Work Health and Safety Act 2011* (Cth).

14.12 Moreover, and specifically in a telecommunications context, both separately and in conjunction with the above recommendations, we strongly recommend that certain telecommunications industry constructs, including wholesale telecommunications services, facilities access arrangements, and software as a service platforms regulated under Schedule 1 of the *Telecommunications Act 1979*, are excluded from reforms relating to the relevant operator concept. This could be through either rule settings, exclusions, exemptions, or clear and unambiguous guidance.

14.13 The facilities access regime, for example, is comprehensive, enforceable and well understood by carriers and those that seek access under this regime.

14.14 The ACCC *Facilities Access Code* (FAC) governs how access to certain telecommunications facilities owned by telecommunications carriers, including mobile towers and underground ducts, is provided to other carriers seeking to install their equipment on or in those facilities. Compliance with the FAC is a carrier license condition, and includes confidential information obligations, the conditions which a Master Access Agreement must contain including access, operation and routine maintenance procedures, confidentiality, technical specifications, rights and obligations in relation to physical access, emergency response procedures, and procedures for access by third party users.

14.15 To capture carriers that are providing facilities access would be duplicative, inefficient, and lead to unnecessary complexity. There may also be limited benefit to any reporting aspects where these entities are already subject to SoCI obligations as responsible entities. This is completely at odds with the objective to reduce unnecessary duplication, complexity, and uncertainty.

14.16 Wholesale telecommunications services where, for example, a Retail Service Provider (RSP) relies on the critical infrastructure of a wholesale broadband provider, would likely see little benefit in identifying the wholesale provider as a relevant operator where the wholesale provider is already a responsible entity under the SoCI framework.

14.17 We support a policy position of proposed exclusions and boundaries which ensure that telecommunications carriage would remain out of scope, and suggests that this is broadened to ensure the policy direction of simplifying the SoCI framework, in alignment with the SoCI Act Review recommendations, remains reflected

in the implementation of the relevant operator concept. Specific and clear exclusions which address aspects particular to the telecommunications industry are necessary to ensuring the effective functioning of the SoCI framework.

15. MEASURE 18 – CORPORATE GROUP COOPERATION

15.1 We support proportionate cooperation obligations within corporate groups where they reflect operational realities and demonstrably enhance security outcomes. However, any such obligations must preserve clear lines of legal accountability and avoid creating uncertainty concerning responsibility, legal professional privilege, confidentiality, or the role of related entities that do not exercise control over the relevant critical infrastructure asset.

15.2 Telecommunications providers often operate across a range of business contexts and legal structures, including data centres, government technology services, telecommunications services, and central corporate functions. The framework should recognise that many organisations regulated under the Act rely on shared systems, services, personnel, and expertise across multiple group entities, while ensuring that legal responsibility remains clearly assigned to the relevant responsible entity.

15.3 Accordingly, any corporate-group cooperation duty should apply only where there is a material operational or security dependency between the entities and the connected entity has a practical capacity to assist the responsible entity in identifying, managing or mitigating the relevant risk. The framework must also expressly preserve legal professional privilege, confidentiality obligations, and appropriate protections for security-sensitive information.

15.4 The proposed connected-entity duty should not apply directly to an offshore affiliate merely because an Australian responsible entity uses a global core network operations platform or centrally managed group cyber security function. While an Australian responsible entity may depend on group-wide IT, security operations centres, identity, and access management, procurement, vendor management or incident response capability controlled elsewhere in the corporate group, that concern is already addressed by the Australian responsible entity's existing obligation to document, govern, assure, and manage those dependencies through its CIRMP, rather than by imposing a new direct Australian civil penalty duty on a foreign-connected entity.

15.5 Direct application to foreign affiliates would create uncertainty and possible conflict with foreign law, confidentiality obligations, and overseas regulatory restrictions. The Consultation Paper acknowledges that practical enforcement against foreign connected entities may depend on Australian presence, assets, conduct, or other jurisdictional connection, and that foreign law and regulatory restrictions must be considered.

15.6 The proposed direct duty may also create perverse security incentives. Global telecommunications groups centralise cyber security, identity management, threat intelligence, network monitoring, and incident response because scale and standardisation can improve resilience and speed of response. A system should not be introduced that may inadvertently fragment operational responsibilities or create Australia-specific processes that reduce the benefits of a unified core security platform. That would be inconsistent with the Consultation Paper's objective of achieving effective security and resilience outcomes rather than procedural compliance for its own sake.

15.7 The Department should further clarify whether a responsible entity would be required to report information received from a connected entity under Part 2D. Any obligation to report information obtained from a connected entity should be confined to clearly defined circumstances in which the information is material to the security of the relevant critical infrastructure asset and is not otherwise required to be reported by the connected entity itself. This would reduce duplication and avoid uncertainty as to which entity bears the primary reporting obligation.

16. MEASURE 19 – SUPPLY CHAIN CYBER SECURITY ASSURANCE

16.1 We support measures to improve cyber security assurance across critical infrastructure supply chains. Supply chain risk is central to the contemporary risk environment, and the proposed measure provides an important opportunity to advance the Review's objective of achieving measurable security outcomes.

16.2 To be effective and proportionate, the framework should adopt a risk-based supply chain assurance model that is not overly prescriptive and is focused on major suppliers and material cyber risks. It should recognise supplier assurances and certifications, accreditations, and existing Commonwealth or internationally standardised assurance evidence where those mechanisms demonstrate equivalent security outcomes.

16.3 Any assurance model also needs to support a responsible entity being able to rely on the assurance activities conducted by their contractors.

16.4 We agree that supplier cyber assurance also needs to be workable in specialised and concentrated supply chains. It is quite common in the telecommunications industry for some suppliers to be the only source of a respective product or service.

16.5 The framework should also distinguish between the supply of active and passive components. Active components may present heightened espionage and foreign ownership, control, or influence risks, whereas risks associated with passive components are more likely to concern continuity of supply in circumstances such as sanctions, trade restrictions, or geopolitical disruption. Assurance requirements should reflect these materially different risk profiles.

16.6 The measure is nevertheless likely to require a substantial uplift in third-party cyber risk management. This may include enhanced vendor risk assessments and supplier assurance processes, supplier audits, contract reviews and amendments, validation of certifications and accreditations, and the ongoing monitoring of critical suppliers. It may also impose additional governance and reporting requirements on major or critical suppliers, increasing their compliance costs and creating a risk that those costs will ultimately be passed on to responsible entities.

16.7 For this reason, the framework should avoid imposing undifferentiated assurance obligations across all suppliers irrespective of their risk profile and should ensure requirements are decided through a lens of what is technically necessary and achievable. Such an approach would increase cost and complexity without necessarily improving security outcomes and would be inconsistent with the Review's central findings. We recognise that cyber security in the supply chain is a critical aspect of the security posture of a telecommunications network. We further support that the framework should allow suppliers and responsible entities to manage cyber security assurance via contractual frameworks. However, further constructive guidance on how this could work operationally is critical to ensure a supplier who supplies to more than one responsible entity is not not forced to implement or manage inconsistent cyber security requirements and/or frameworks across the same product or services lines.

16.8 There also appears to be some duplication between these proposals and those relating to relevant operators in Measure 17. If both measures are pursued, the legislation ought to include clear 'anti-overlap provisions' to ensure that the reforms do not give rise to duplicative or overlapping obligations.

17. MEASURE 20 – SPECIFIED RISK INFORMATION

17.1 We support the Government having access to the information necessary to understand and manage material national security and critical infrastructure risks. However, any power relating to specified risk information must be appropriately targeted, proportionate, and accompanied by robust safeguards for commercially

sensitive, security-sensitive, and customer-confidential information.

17.2 The Department should clearly define the categories of information that may be requested and require each request to satisfy tests of necessity and proportionality. The framework should also specify how information provided by responsible entities will be stored, used, shared, and protected by the Government.

17.3 Greater clarity is required regarding the circumstances in which the Secretary may issue specified risk information, the anticipated frequency of such notices, whether notices will be issued through a single authoritative source, and how they are intended to differ from non-binding guidance. The practical burden imposed on responsible entities will depend significantly on the frequency, volume, and manner in which such information is provided.

17.4 We consider that any notice should be issued directly by the Secretary, in writing, and specifically addressed to the responsible entity concerned. Reliance on a self-service website or similar mechanism would create a risk that important notices are overlooked and would provide insufficient certainty as to when an obligation has been triggered.

17.5 Subject to the urgency of the relevant risk, responsible entities should ordinarily be given six months to consider and assess the specified risk information and to implement any necessary measures. A further two months should then be allowed for the entity to provide a brief written response outlining its assessment and indicating whether action has been taken, is not considered necessary, or is planned, together with the proposed timeframe for implementation where it could not be achieved in the initial two month timeframe. Shorter periods may be appropriate where the notice concerns an urgent or immediate risk.

17.6 In designing these obligations, the Department should recognise the considerable differences in capability and resourcing across regulated entities. Any requirement to review or respond to specified risk information should therefore be targeted, proportionate, and reasonably capable of implementation by small and medium-sized entities.

17.7 Information powers ought not create overlapping reporting obligations or require responsible entities repeatedly to provide information that is already available to the Government through other regulatory processes. Avoiding such duplication would be directly consistent with the Review's findings concerning regulatory complexity and overlap.

17.8 Where a notice relates to a risk already addressed by an overlapping legal or regulatory requirement, the Department ought to identify that requirement when issuing the notice. Responsible entities ought to be permitted to respond by demonstrating compliance with the existing obligation, rather than being required to undertake or report on duplicative measures.

18. MEASURE 21 – CRITICAL WORKERS AND CRITICAL COMPONENTS

18.1 We support the identification of critical workers and critical components as an important element of national resilience. However, the reforms must account for workforce shortages, limitations in vetting and clearance capacity, and the practical realities of operating secure digital infrastructure.

18.2 Critical-worker obligations should be risk-based, role-specific, and aligned with existing personnel-security frameworks. This should include recognition of the Defence Industry Security Program, Facilities Access Code (FAC), requirements imposed by customers that are aligned with the Protective Security Policy Framework, and Australian Government Security Vetting Agency clearance processes, where relevant.

18.3 The proposed amendments, which would replace the existing definition of a critical worker, are likely to alter both the individuals who fall within that definition and the corresponding checking, monitoring, and access-control obligations. Responsible entities would therefore need to reassess their workforces against the revised definition and take any necessary steps to comply with their CIRMP obligations.

18.4 This reassessment would extend beyond a responsible entity's direct employees to relevant personnel engaged by operators, connected entities, managed service providers, contractors, and subcontractors. For entities with large or geographically dispersed workforces, extensive supply chains, or complex outsourcing arrangements, this would represent a substantial undertaking. Identifying all potentially affected individuals may itself take several months and result in increased administrative activities. The costs of such increased activities will likely be passed on to responsible entities.

18.5 The framework should avoid imposing broad personnel-security obligations that exacerbate existing shortages in cyber security, cloud, engineering, and security-cleared technical roles. It should instead provide clear definitions, practical transitional arrangements, and appropriate recognition of existing vetting and assurance processes.

18.6 Personnel engaged by third-party service providers should not be classified as critical workers where they have no direct access to, or practical ability to interact with, live data or operational systems. The definition should be directed to roles that present a material security risk, rather than capturing individuals solely because they provide services to a responsible entity.

18.7 The requirements should also not be framed or applied in a manner that directly or indirectly requires the onshoring of functions. Many technology services rely on offshore support to provide continuous 'follow-the-sun' coverage, and the framework should preserve the ability to use such operating models where risks are appropriately managed.

18.8 Telecommunications providers commonly rely on extensive supplier networks, with suppliers often engaging their own subcontractors. A responsible entity should therefore be permitted to rely on background checks and suitability assessments undertaken by a third party, rather than being required to repeat those checks itself.

18.9 Any assurance arrangements supporting such reliance should be straightforward and inexpensive. For example, the third party could provide an attestation confirming that the necessary checks and assessments have been completed, and that any ongoing monitoring requirements are being met. The responsible entity should not be required to obtain copies of the underlying background checks or suitability assessments, given the duplication and significant privacy implications this would entail without a commensurate security benefit.

18.10 A minimum transitional period of 12 months should apply to the implementation of the reforms. A staged approach would also be appropriate: the revised requirements could apply to individuals newly appointed to relevant roles from six months after commencement, while existing personnel should be given 12 months from commencement to complete any required checks. Any future amendments should likewise be accompanied by sufficient time for regulated entities to transition their arrangements.

18.11 In relation to critical components, definitions should focus on function and consequence rather than asset category alone. A component should be treated as critical only where its compromise would materially affect the availability, integrity, reliability, or security of a critical infrastructure asset or function.

18.12 We caution against designating particular components as critical through prescriptive rules where the designation may not reflect their actual operational significance. An overly prescriptive approach could result in components being treated as critical despite presenting no material risk in a particular technological or operational context.

18.13 Responsible entities must retain sufficient flexibility to identify critical components by reference to their own systems, architecture and risk environment. Prescriptive rules are unlikely to adapt effectively to technological change or the diverse operating contexts of regulated entities and may impose additional compliance costs without improving the security of critical infrastructure.

18.14 We support the provision of greater certainty and guidance on the identification of critical components. However, this should be achieved through sector-specific guidance rather than prescriptive rules. Sector-specific definitions and guidance should be co-designed with industry, drawing on the successful collaborative approach used in developing the original Telecommunications Security and Risk Management

Program Rules

Ends

Australian
Telecommunications
Alliance

Level 25 / 100 Mount Street
North Sydney NSW 2060

T 02 9959 9111
E info@austelco.org.au
W austelco.org.au

ABN 56 078 026 507