COMMUNICATIONS
ALLIANCE LTD

Communications Alliance submission

to the

Department of Home Affairs
Consultation Paper

Protecting Critical Infrastructure and Systems of National Significance

16 September 2020

Page intentionally left blank.

1. Introduction

Communications Alliance* welcomes the opportunity to provide a submission in response to the Department of Home Affairs (Department) Consultation *Paper Protecting Critical Infrastructure and Systems of National Significance*.

In our submission, we have not responded to all the questions posed in the Consultation Paper but rather offer some general observations that will go to many of the points raised in the Paper.

As with previous reforms in relation to Australia's national security, the communications and data/cloud sectors are keen to assist Government to ensure that, to the extent possible, Australia's critical infrastructure is secure and resilient in the face of natural disasters and other hazards, and appropriate processes are in place to cope with actual threats to and attacks on our sector's critical infrastructure.

Our sector already has extensive experience in collaborating effectively with Government, security agencies and regulators across a number of regulatory and legislative instruments and frameworks, e.g. assistance provided to law enforcement agencies under the *Telecommunications Act 1997*, the protection of critical infrastructure, including supply chains, in accordance with the Telecommunications Sector Security Reforms, the Data Retention Regime and the *Assistance and Access Act 2018*, just to mention a few. Our sector also extensively engages with emergency services organisations and Federal Government and State/Territory departments in relation to natural disasters and the COVID-19 pandemic.

We are conscious that the protection of critical infrastructure is a national priority and, as such, must also be tackled through a collaborative approach across all sectors and stakeholders.

About Communications Alliance

Communications Alliance is the primary telecommunications industry body in Australia. Its membership is drawn from a wide cross-section of the communications industry, including carriers, carriage and internet service providers, content providers, equipment vendors, IT companies, consultants and business groups.

Its vision is to provide a unified voice for the telecommunications industry and to lead it into the next generation of converging networks, technologies and services. The prime mission of Communications Alliance is to promote the growth of the Australian communications industry and the protection of consumer interests by fostering the highest standards of business ethics and behaviour through industry self-governance. For more details about Communications Alliance, see http://www.commsalliance.com.au.

***NOTES:**

nbn™ is a member of Communications Alliance but has not been involved in the preparation of this submission.

Communications Alliance members, including those with interests in the space and data/cloud sectors, may prepare additional feedback in individual submissions to the Department.

2. Principles-based outcome approach

There can be no doubt that significant parts of Australia's telecommunications infrastructure are critical to the functioning of the country's economy and society. Indeed, the recent bushfire season and, of course, the COVID-19 pandemic, have underscored the critical nature of our sector's infrastructure.

The criticality of this infrastructure has long been recognised and, consequently, telecommunications-specific legislation and regulation that aim at protecting this infrastructure and the data and communications that travel across it have successively been expanded or introduced over the past decade.

Similarly, existing legislation and regulation also recognises the assistance that the telecommunications sector can (and does) provide for the protection of national security and for law enforcement purposes.

We note our sector has also a long history of actively maintaining and further developing an all-hazards-approach with respect to the security of telecommunications networks.

In summary, of all the sectors considered by the Department in the Consultation Paper, we believe that the telecommunications industry is presently the most comprehensively regulated from a security perspective. We have no evidence that would suggest that the existing regulations are failing and that our sector is not adequately protecting its infrastructure with respect to physical, cyber, personnel or supply chain security.

Against this background, we welcome the proposal to focus on "a set of principles-based outcomes across Australia's critical infrastructure sectors to protect critical entities from all-hazards."[1]

Across sectors, principles-based security obligations are a proportionate response to existing and foreseeable threats and provide an important ability for each entity to customise its respective risk-management approach in accordance with its sector, technologies used and specific context.

The proposed principles-based outcomes, designed to give effect to the Positive Security Obligation (PSO) appear sufficiently broad to be able to retain significance and currency in an environment – such as the telecommunications sector – that is characterised by rapid changes in technology and user behaviour. As far as we are able to comment, the proposed outcomes also appear to form an appropriate basis for the other critical infrastructure sectors considered in the Consultation Paper.

In addition to stipulating outcomes-based principles, it will be equally important to clearly establish criteria in the legislation, at a high level, against which any measures contemplated in subordinate instruments of regulation, industry codes, standards, guidelines etc. can be developed and measured. Such criteria ought to include

- the necessity of the measure;
- its proportionality, including in relation to any attendant costs of the measure;
- its effectiveness;
- its technical feasibility;
- the legitimate interests of the critical infrastructure entity;
- the availability of other means to achieve the desired outcome;
- the intrusiveness of the measure, any implications for privacy and whether less intrusive measures could be equally effective; and

[1] p. 17, Department of Home Affairs, *Protecting Critical Infrastructure and Systems of National Significance*, Consultation Paper, August 2020

- the need for a scheduled review as to whether the measure remains appropriate.

As indicated above and explained in further detail below, telecommunications carriers already operate effectively under a principles-based framework – most notably the *Telecommunications Sector Security Reforms* (TSSR) as part of the *Telecommunications Act 1997* (Telecommunications Act) – to prevent and respond to security threats.

Therefore, we welcome the Department's intention to "work with critical infrastructure entities to ensure that the reforms are developed and implemented in a manner that secures appropriate outcomes without imposing unnecessary or disproportionate regulatory burden, in accordance with guidance from the Department of Prime Minister and Cabinet's Office of Best Practice Regulation."[2]

Consequently, in sectors such as telecommunications, where there is a well-established security framework in place, the translation of principles-based outcomes ought to be sector-specific and any existing legislation ought only to be augmented if there is evidence that further measures are required.

3. Advanced legislative and regulatory framework in the telecommunications sector

In 2018, significant security requirements were enshrined in telecommunications legislation via the TSSR, which were developed through industry/government collaboration and have been operating for almost the past two years. There is also a range of other telecommunications sector-specific legislative instruments and regulation that is relevant to security and an all-hazards approach in the sector.

There are many security-related obligations that have been imposed over the past few years that relate to our sector. While arguably individually necessary, the impact of these increasing obligations needs to be considered in aggregate before decisions are made as to whether to impose new obligations. More time ought to be afforded to judge the competitive, commercial, economic and social impacts of the significant changes proposed.

Although there has not yet been sufficient time for exhaustive analysis, we believe for a number of reasons that, to the extent necessary, building on the foundations of the Telecommunications Act and TSSR clearly is preferable to the alternative (i.e. moving existing obligations into the planned amended *Security of Critical Infrastructure Act 2018* (SoCI Act) and building additional regulations and obligations under that framework).

These reasons include that the former approach:

- can be advanced more rapidly: time and effort need not be spent on the re-design of existing frameworks, nor on managing the inevitable disruption;
- will be more cost-effective: a simpler overall framework, managing fewer pieces of legislation, fewer regulators and other stakeholders will exhaust fewer resources overall; and
- recognises that the telecommunications industry already complies with a mature security framework: C/CSPs have learned how to manage requirements and obligations under TSSR and the Telecommunications Act and can build from that known base more readily than starting anew under a different framework.

The existing framework is flexible and was established for this purpose. There are longstanding provisions under the Telecommunications Act that can be used to achieve Government's policy objectives – these should be explored, rather than new mechanisms created.

[2] p.10, ibid

An initial high-level analysis of the proposed reforms indicates that the existing legislative framework for telecommunications already contains – and the industry complies with – a number of the proposed obligations.

While TSSR may be the most widely known aspect of legislation for our sector, the Telecommunications Act and other regulatory instruments contain important additional obligations and options for implementation of the proposed reforms, including where those proposals target all hazards.

Part 13 of the Telecommunications Act sets out the obligation to do the "carrier's best or the provider's best to protect telecommunications networks and facilities owned, operated or used by the carrier or provider from unauthorised interference or unauthorised access"[3] and to "give […] help as is reasonably necessary"[4] to officers and authorities of the Commonwealth and of the States and Territories (along with complementary immunity and 'no profit no loss' provisions) and includes the far-reaching TSSR protection, notification and approval requirements. We note that these obligations are not cyber security-specific, but go to broader obligations to protect networks.

Part 13 also provides for the suspension of services in emergencies.

Part 16 of the Telecommunications Act deals in part with responses to disasters and civil emergencies and could be used to incorporate other specific obligations rapidly.

Part 6 of the Telecommunications Act already provides a framework for the development of enforceable industry Codes and Standards.

Moreover, other mechanisms in the Telecommunications Act can be used to implement Government's policy objectives (including carrier licence conditions and service provider rules) rather than the creation of a whole new framework. We also note that the underlying philosophy of the Telecommunications Act is one of co-regulation – the industry should be given the opportunity to develop industry generated codes and standards (which have force of law).

It is also worth highlighting that the telecommunications sector already has a framework of instruments and arrangements for an all-hazards approach to managing critical infrastructure impacts.

These include the:

- Emergency Call Service Requirements Code, dealing with protection of Triple Zero services, including in a cyber event (enforced by the ACMA);
- Triple Zero protocol that deals with all hazards that disrupt Triple Zero capability;
- Scam Reduction Industry Code (awaiting registration by the ACMA) that combats scam traffic impacts on networks and consumers;
- an all-hazards Communications Protocol for managing telecommunications disruptions due to major emergency events;
- operation of the Communications Sector Group (a sub-group of the TISN), co-chaired by TPG Telecom; and
- the potential for disaster plans or network survivability plans under Part 16 of the Telecommunications Act.

The sector is also focused on new arrangements for creating stronger communications infrastructure resilience capability – e.g. via additional back-up generators, cells-on-wheels (COWs) etc – in the wake of the 2019-20 bushfire events.

Against this background, we welcome the Consultation Paper's statement: "Government will work in partnership with critical infrastructure entities to ensure the new requirements build on

[3] Part 13, Section 313 (1A), *Telecommunications Act 1997*
[4] Part 13, Section 313 (3), *Telecommunications Act 1997*

and do not duplicate existing regulatory frameworks. This approach recognises that many operators of critical infrastructure, particularly in the banking, finance, aviation, maritime and communications sectors already operate under regulatory frameworks that impose risk management, report and transparency obligations. Regulators in those sectors are already equipped to supervise those entities, identify emerging threats, and assist regulated entities respond to those threats. By focusing on outcomes, the new framework will ensure consistent security standards across all sectors without unnecessary regulator impost."[5] Indeed, we recommend the inclusion of a statement of intent to this effect into the legislation to provide guidance to regulators and other authorities with regard to the development of sector-specific rules frameworks.

Consequently, in light of the advanced state of legislation, regulation and voluntary industry efforts for the protection of critical infrastructure, we call on the Department to perform a thorough and evidence-based 'gap analysis' of the proposed principles-based outcomes and contemplated measure vis-à-vis the existing obligations and practice in the telecommunications sector and the extent to which those achieve the outcomes considered in the Consultation Paper. This would be a far more useful exercise than the Regulation Impact Statement (RIS) that is being prepared during the current consultation period and which – in the absence of any clarity as to the specific planned legislative provisions or subsequent regulations – cannot produce any credible guidance.

If, subsequent to such a gap analysis, there is evidence that further regulatory change for the telecommunications sector is a reasonable, necessary, effective and a proportionate response to the dynamic threat environment, then our industry believes that the best option to cement the desired PSO and any further enhanced security obligations and assistance in our sector would be to build on the solid existing foundations of the Telecommunications Act (including TSSR) and industry regulation.

In line with the above, we believe that the regulators for our industry ought to remain as currently prescribed in the respective legislation/regulation, i.e. the Australian Communications and Media Authority (ACMA) and, to the extent notification and approval under the TSSR are concerned, the Critical Information Centre ought to continue to exercise their respective functions to monitor and enforce the security obligations under which our sector operates.

It has been noted that some critical infrastructure entities are operating across several sectors and the resultant need for the proposed reforms to allow such entities to 'aggregate' requirements placed upon them, or at least not be confronted with conflicting requirements. We believe that this would be best facilitated with a principles-based approach that allows entities engaging across two or more critical infrastructure sectors to design strategies and measures specific to their cross-sector challenges. Such an approach already appears to have been considered with communications related 'space' assets being excluded from the space sector. A similar approach should be taken to 'data and the cloud' sector to ensure that any proposed regulatory approach is fit-for-purpose and does not create a duplicated regulatory impetus on already regulated communication assets. These principles ought to be supplemented by clear guidance as to how compliance with the principles could be achieved but with a clear view to remaining open to alternative approaches that achieve the desired outcome. The fact that some entities operate across sectors does not negate the need for and the superiority of a sector-specific approach to the reforms.

4. Enhanced cooperation and resilience strategy

The Consultation Paper raises the question as to whether and how a revised Trusted Information Sharing Network (TISN) and Critical Infrastructure Resilience Strategy could support the proposed reforms.

[5] p. 12, Department of Home Affairs, *Protecting Critical Infrastructure and Systems of National Significance*, Consultation Paper, August 2020

Our sector welcomes the proposal to revitalise TISN and the Critical Infrastructure Resilience Strategy. A renewed TISN and Resilience Strategy could assist by receiving and reviewing security incidents and report back to the Communications Security Group (CSG) on key threats, patterns and trends.

A revised TISN model could take on similar structures to the current arrangements, however with improved resourcing, and representation from data centres which are a key component of today's communications environment.

We also note that Government has a critical role to play in facilitating cross-sectoral collaboration on security and resilience. Recent crises have highlighted that additional Government assistance for the building and maintenance of cross-sectoral relationships between critical infrastructure sectors, or indeed entities, would be beneficial. These include (but are not limited to) cooperation between the telecommunications, energy and transport/logistics sectors.

The telecommunications sector has already taken significant steps in this direction and is engaging closely with the energy sector. However, more consistent and multi-lateral formalised arrangements (processes and protocols) ought to be developed, facilitated by Government agencies. Consequently, the 'Playbook' of response plans for a range of scenarios contemplated in the Consultation Paper also ought to be cross-sectoral rather than remain sector-specific. This does not imply that it would be necessary, or indeed desirable, to assimilate the specific rules for implementation of the new reforms – specific implementation rules ought to be avoided as far as possible in favour of a principles based approach – but rather highlights the need for improved cooperation across sectors in preparation for and during disasters.

Moreover, it would also be beneficial if Government assisted industry efforts by analysing and promoting awareness (including within Government itself) of the upstream impact of communications outages on the economy – including for the finance sector, mining/resources and Government's own network and resources.

The Consultation Paper also proposes improving situational awareness through enhanced threat sharing mechanisms. The Cyber Security Strategy 2020 allocates $35.3M to a cyber threat sharing platform. The Strategy also foreshadows the investment of "$62.3 million in a classified national situational awareness capability to better enable government to understand and respond to cyber threats to critical infrastructure and other high priority networks. This will be complemented by increased incident reporting and near-real-time threat information from the most essential pieces of infrastructure as part of future regulatory requirements."[6] Similar proposals to receive near-real time information about networks and systems are contained in the Consultation Paper.

Our members have repeatedly called for an advancement in threat-sharing mechanisms and, consequently, welcome Government's commitment to further improve existing arrangements and to devote funding to this cause. However, without a better understanding as to what information would be required of critical infrastructure operators (which is not already being provided under current legislation), it is difficult for our sector to provide more specific feedback, including on the adequacy of funding and suggested timeframes, on this proposal.

In this context we also note that it would be beneficial to take a wider perspective on close cooperation, and indeed coordination, with respect to cyber security, national security and online safety. For example, Internet Service Providers also work (under various legislative frameworks) with different Government agencies and regulators to limit access to certain online locations and content. These arrangements ought to be centralised and automated to streamline operations and minimise the risk of error, including in online crisis events. The proposed threat sharing efforts ought to include funding for such arrangements.

[6] Item 37, p. 23, Department of Home Affairs, *Australia's Cyber Security Strategy 2020*, August 2020

5. Systems of National Significance

The Consultation Paper appears to propose potentially far-reaching reforms. As indicated above, the telecommunications sector is already well-advanced with respect to legislative, regulatory and industry-driven efforts to protect its networks and, consequently, many elements of the proposed reforms may find a greater application in less 'advanced' critical infrastructure sectors of the Australian economy.

In order to provide meaningful feedback on the reforms and their translation into legislation, a greater degree of clarity as to what is actually being proposed for our sector would be required at an early stage in the process.

For example, it is not clear which entities in our sector would be considered operating 'Systems of National Significance' (SoNS) and which entities would fall under the category of 'Regulated Critical Infrastructure Entities' (RCIE). Similarly, where an RCIE operates one or more SoNS as well as (non-SoNS) regulated critical infrastructure, it is unclear how the obligations relating to the SoNS of that entity are delineated from other critical infrastructure owned and/or operated by the RCIA. Ggiven the far-reaching obligations for those entities, it will be key to get a clear understanding of those definitions, and the resultant 'mapping' of entities to categories, earlier (i.e. now) rather than later in the process. This will allow our industry to more effectively work with Government on implementing the principles-based outcomes for our sector.

For example, it is not clear whether threshold criteria such as size or geographic location or reach will be applied to the definition of SoNS. Similarly, consideration would need to be given to large IoT-based sensing networks and their respective devices: would those be considered SoNS and, if so, to whom and at what layer would the obligations apply? For example, it is not unlikely that the responsibility for the physical security of sensing devices would lie with one entity while the transmission of the data is being handled by another entity, with the security of the software controlling the device being handled by yet another entity.

6. Directions and direct action

Of great concern is the 'direct action' power envisaged to be given to Government agencies. While we have, unfortunately, not been able to gain a better understanding as to what such powers entail and how those would be translated into regulation in the telecommunications and data/cloud sectors (to the extent this was deemed necessary after a thorough gap analysis), we highlight the inherent risks that may be attendant to a direct action power. A number of issues are to be considered in this respect, including

The direction and direct action powers, which may 'override' an operator's property and ownership rights over assets and infrastructure, require careful consideration of a variety of issues, including

- Who/which agency would be receiving these powers;
- How will advice prior to the use of these powers be sought;
- Requirements for consultation;
- Independent authorisation;
- Other oversight, governance and reporting arrangements;
- Time limits and possible emergency exercise of powers;
- Duration of the assistance/direct action;
- Technical capability of the respective agency;

- Possible damage to operators' infrastructure as a result of directions/direct action; and
- Immunities and/or indemnities

We comment on some of these below:

The Consultation Paper notes "Government's unique understanding of Australia's threat environment and the interdependencies within critical infrastructure sectors [which] position it best [to] determine appropriate preventative actions and resource allocation in a crisis."[7] The Paper also highlights Government's role "to use its enhanced threat picture and unique capabilities to take **direct action** to protect a critical infrastructure entity or system in the national interest."[8]

We recognise Government's sophisticated capabilities in gathering and analysing intelligence in relation to cyber threats emanating nationally and internationally. However, we believe that the determination of preventative actions and resource allocation, including across sectors, in a crisis is and must remain a joint industry-Government exercise. Or to put it differently, if Government was indeed best placed to determine such action, then the existing (and to be revitalised) cooperation mechanisms between industry and Government and across sectors cannot be deemed to work satisfactorily and ought to be improved to ensure that both, industry and Government are – jointly – positioned to appropriately deal with acute cyber incidents.

Similarly, we cannot envisage a scenario – even during an 'immediate and serious cyber threat' – in which a Government agency would be *better* placed than the operator of critical infrastructure (including in the data/cloud sector) to take direct action to protect the infrastructure or system. The complexity and dynamic nature of the systems (including software-defined networks) necessitate reliance on the expertise of the operator of the system (or the customer of the data/cloud system), especially in times of crises where time is likely to be of the essence and decisions need to be taken under significant pressure.

The powers to issue directions and to take direct action must be subject to stringent and independent governance arrangements and should apply in only the rarest of situations: such as in the (almost unthinkable) circumstance in which an operator refused to cooperate with Government in a That is this power should not derive from a belief that Government is better placed to take action but rather from an absence of the preferable alternative – that action be taken by the operator. Moreover, direct action should only be contemplated after the operator has failed to comply with a direction.

Any directions and direct action ought to be approved by an independent judicial authority which has access to expert technical advice. In determining whether approval ought to be granted, the authority ought to have regard to a variety of factors. Those factors include the items mentioned in the Consultation Paper (wider consequences, potential for spread, imminence of the threat) but must also extend to an analysis of the risks of 'getting it wrong', i.e. the risk of unintended consequences for the system and any upstream use of the system.

Therefore, we propose that Government adopt and implement the recommendations[9] that the Independent National Security Legislation Monitor (INSLM) recently made in relation to similar powers that arise from the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* – for the purpose of that Act as well as for the purpose of directions and direct action powers under the proposed reforms. Any immunities

[7] p. 28, Department of Home Affairs, *Protecting Critical Infrastructure and Systems of National Significance*, Consultation Paper, August 2020
[8] p. 29, ibid
[9] The INSLM recommended that the approval of far-reaching powers under the *Assistance and Access Act 2018* be vested in a newly created Investigatory Powers Division (IPD) within the Australian Appeals Tribunal (AAT). The INSLM further recommended that this IPD be headed by a retired judge of the Federal Court or the Supreme Court of a State or Territory (appointed by the Governor-General, on the advice of the Attorney-General, following mandatory consultation on the appointment with the Leader of the Opposition) and receive expert advice from imminent lawyers and technical experts. The full text of the INSLM's recommendations can be accessed in his Report *Trust But Verify*.

contemplated for Government agencies also ought to extend to the operator subject to the direction or direct action.

7. Standards and supply chain considerations

As previously noted, we support a gap analysis of the current TSSR assessment process for supply chain risks for carriers and other critical infrastructure entities to be undertaken as a priority. If such an analysis finds any gaps, the telecommunications industry stands ready to assess how existing global standards could assist with closing the identified gaps.

Given supply chains that support communications networks in Australia are global in nature, as are many networks themselves, it is critical to consider replicating existing international standards as they apply across the supply chain.

Generally speaking and without prejudice to the required gap analysis outlined above, our industry supports global efforts towards a standardised security development and solution design, referred to as Security Assurance Methodology (SECAM).[10] There is a real risk that uncoordinated global efforts in this area will lead to a diverging set of security requirements, which would jeopardise not only interoperability, but make security that much more complex to guarantee.

Global standards and best practices are fundamental to the efficient handling of threats – especially given that a large share originate across national borders – as well as to building economies of scale, avoiding fragmentation and ensuring interoperability. Therefore, it is essential that stakeholders, including operators, vendors, regulators, policymakers and IT-focused companies as well as players from other industries, work together to set common and open security standards that specify what needs to be secure and protected, rather than mandate the use of a particular technology. That is the telecommunications industry does not support fragmented, prescriptive national certification schemes for devices and IT systems, or expensive, time consuming certifications like, for example, the Defence Level Common Criteria (CC).

Beyond a gap analysis, our members seek clarification on if and how the inclusion of new co-designed supply chain principles will be imbedded into Government decision making process and suppliers to support competition and diversity in the market.

8. Process and Timeframes

As previously indicated and highlighted during the ongoing consultation, the Consultation Paper significantly lacks detail as to what the reforms actual entail and how specific concept translate into obligations for critical infrastructure entities.

We recognise that the Paper seeks input from all sectors with regard to most of the specific aspects of the reform. However, we note that if such feedback is to be meaningful, it needs to be informed through debate.

By way of comparison, consultation around and development of the TSSR spanned four years and involved three exposure drafts, followed by consultation on guidelines and technical implementation. Similarly, the development of the Data Retention Regime also included consultation on an exposure draft of the proposed legislation and the establishment of a Data Retention Implementation Working Group which brought together expertise from various stakeholders produced consensus recommendations that were

[10] Security Assurance Methodology (SECAM) establishes security requirements not just for products but also for product development processes. According to proposed SECAM rules, accreditors will verify a 3GPP manufacturer's overall capability to produce products that meet a given set of security requirements, which will eliminate the need for explicit certification on a per product basis, while also encouraging a solution based view.

accepted by Government, and productively shaped the mechanics and specifics of implementation.

While we recognise that Government sees an urgent need for reform, especially for sectors less advanced than the telecommunications sector from a security perspective, we believe that more extensive consultation, particularly with respect to the specific requirements envisaged for individual sectors, is required to ensure that the reforms create a practical, effective and proportionate framework.

The timeframes conveyed to industry during the consultation process (legislation to be introduced into Parliament in Sept-Dec 2020; design of sector-specific standards from late 2020 to early 2021; obligations effective in mid-2021) appear significantly too short and ought to be revisited.

We welcome the decision to provide relevant stakeholders with an Exposure Draft of the legislation (as foreshadowed in recent discussions with Government) and urge Government to carefully consider any feedback received during the consultation process on the Exposure Draft.

To further allow for constructive engagement over the sector-specific approaches to implementing the reforms we strongly recommend that a Critical Infrastructure Implementation Working Group (CIIWG) be created which brings together experts from Government, security agencies, industry experts from the critical infrastructure sectors, regulators and other relevant stakeholders. The CIIWG (and potentially sector-specific sub-groups) ought to be working to develop an effective, proportionate and practical implementation path for critical infrastructure sectors.

A similar working group was formed during the development of the Data Retention legislation and implementation phase and provided, so we believe, constructive and valuable input into the legislative and implementation process.

This Working Group (or Government) also ought to identify and clearly articulate any desired outcomes of the reforms, the timeframes to achieve those outcomes and the current baseline/status of individual 'work items'. It is equally key to understand how progress and success for each target outcome will be measured and reported against.

<u>Approach to data/cloud sector</u>

With respect to the data/cloud sector we note that, given the complexity and broad definition of 'cloud', the regulatory intent for Cloud Service Providers must be clearly laid out and understood. These service providers offer a wide variety of products and the breadth of their customers is vast, thus the build-out of the sector-specific guidance and framework for this sector must be a considered process. We recommend that Government first undertake the guidance and framework design for each other sector and only undertake the drafting of guidance and rules, to the extent required, for the data/cloud sector once the overlay of already existing regulatory onus for data and cloud are fully understood. Therefore, prior to any measures being finalised, a thorough gap analysis of the proposed principles-based outcomes and contemplated measures versus existing obligations across the various sectors to which cloud providers offer services ought to be undertaken. Doing so will assist with ensuring that Government's objective of avoiding unnecessary duplication and regulation can be met.

To the extent that data/cloud constitutes its own industry vertical (rather than being a horizontal enabler across all sectors), it will be useful to concentrate thinking on practical guidance for the security of data independent of its location, i.e. irrespective of whether data is being stored on-premise or in the cloud.

Similar to our comments in relation to supply chain considerations (Section 7), we note that the data/cloud sector is already using a range of international security standards, e.g. ISO27001 Series, SOC 1, 2 and 3 and PCI DSS, and frameworks such as ISM and IRAP. The use

of existing standards, which are already used by a number of global organisations, must be a priority in order to avoid unnecessary complexity for this sector.

We envisage that the recommended CIIWG would also be able to provide valuable assistance with the data/cloud piece.

Cost-benefit analysis – Regulatory Impact Statement

Our industry recognises the need to for a cost-benefit analysis of the proposed critical infrastructure reforms and appreciate any consideration that has been given to this matter as part of the development of a Regulatory Impact Statement (RIS) thus far.

We are keen to assist Government with developing an understanding of the costs that the communications sector will incur as a result of the proposed reforms to allow scenario/options-modelling and inform evidence-based decision making.

Unfortunately, given the timing of the Regulatory Impact Statement and the lack of clarity on scope and detail of the proposed reforms, critical infrastructure entities are not in the position to provide meaningful compliance cost estimates at this stage. The costs that our members (and our sector more generally) are likely to incur are largely dependent on two factors:

- the extent to which the proposed reforms use and build on existing legislation and regulation in our sector (e.g. TSSR, Telecommunications Act, existing industry codes etc.) as opposed to creating a new legislative regime under the SoCI Act 2018; and
- the detail of what is actually required of our sector, with such detail being contained in the regulations that are foreshadowed to be developed after the passage of the legislation underlying these sector-specific regulatory instruments.

We also note that the compliance cost estimates that have been presented to us in the course of the ongoing consultation, which were collected through online literature review, are highly unlikely to be useful in this context:

- The figures presented are derived from international comparison and would, therefore, need to be adjusted to reflect the Australian market, underlying technologies and legislative/regulatory framework. It is not clear how this could be done;
- The figures also reflect overall regulatory compliance costs rather than being specific to national security or cyber security; and
- The figures are also unlikely to be sufficiently recent given the rapid technological change of our sector and given they are derived from literature review rather than recent first-hand interviews or other recent, directly-sourced information.

The combination of these factors mean that it is, in our view, impossible to meaningfully derive costs estimates for the Australian communications sector from the numbers that have been researched and, therefore, they ought not be used for the purpose of a RIS.

We would be happy to attempt to provide cost estimates once the legislative basis of the reforms has been developed and we have greater clarity of the underlying sector-specific requirements and regulations.

9. Conclusion

Communications Alliance looks forward to continued engagement with the Department of Home Affairs and other relevant stakeholders on this important topic.

We share Government's desire to create a robust, effective and efficient framework that appropriately protects Australia's critical infrastructure and systems of national significance.

To the largest extent possible and only to the extent required, this framework ought to build on and enhance existing legislative frameworks and industry efforts. A thorough and evidence-based gap analysis is required to ensure the reforms are not duplicative or, worse, contradicting existing frameworks.

Our members stand ready to work with Government and all other relevant stakeholders to create a practical, effective and proportionate framework in a realistic timeframe.

For any questions relating to this submission please contact Christiane Gillespie-Jones on 02 9959 9118 or at c.gillespiejones@commsalliance.com.au.

Published by:
COMMUNICATIONS
ALLIANCE LTD

Level 12
75 Miller Street
North Sydney
NSW 2060 Australia

Correspondence
PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
E info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507