Telecommunications Security Review
Department of Infrastructure, Transport, Regional Development and Communication
GPO Box 594
Canberra ACT 2601
Australia

29th March 2022

Re: Proposed Instruments to enhance Security information obligations for carriers and eligible carriage service providers

To whom it may concern:

Thank you for the opportunity to provide comment and input on proposed legislative instruments that will impose security information obligations on carriers and eligible carriage service providers.

Real World Group, comprising of Real World Networks Pty Ltd (Carrier License 386), Real World Technology Solutions (CSP), Industrious Partners Pty Ltd (CSP) and Blueteq Pty Ltd, is a national telecommunications provider. We provide wholesale and retail telecommunications services, along with managed IT and Network infrastructure and cyber security consulting to a range of end users, including industry and government customers.

With reference to the current global security environment, and the prevalence of cyber-security threats, we understand the necessity of rules such as these to help ensure that our critical national communications infrastructure remains secure, stable, and operational. We welcome the government's willingness to engage with industry to improve security practices, and the efforts the department has undertaken to engage and communicate regarding the proposed instruments.

We do however retain some concerns over the proposed conditions and would encourage the department to find mechanisms to address these prior to introducing the instruments in the coming weeks. In particular, we note that the current wording will have broad unintended consequences as it does not sufficiently define the instrument's intended scope.

Grouping of Carriers and CSPs
As currently drafted, the various instruments will require the provision of separate reports and asset lists from each Carrier and CSP, even if they are within a corporate group – such as within our group. In many cases the complex network of internal business relationships will result in a substantial amount of duplicated effort, as well as significant complications in how asset information is stored and reflected internally to support the requirements.

A more sensible approach would be to allow an entity comprising of one or more Carriers or Carriage Service Providers to designate a responsible Carrier or CSP as the designated reporting entity for the group. Similar mechanisms already exist under other aspects of telecommunications legislation, and it would seem reasonable that such rules could be extended here.

Scope of definition of Cyber Security
A primary concern of the proposed instruments is the definition of a 'cyber security incident'. While the department's industry briefing made it clear that the intention was to only capture events where there is a 'cyber' attack (specifically referred to as containing a Software element) the currently proposed definition is a lot broader and captures incidents outside the instruments' intended scope.

In reviewing network incidents from the past 24 months, we have identified a number of events that we understand are not intended to be covered by the scope of this determination but would in fact be captured by the currently proposed definition of an incident; because the scope is only limited by the fact that the action is unauthorised, and the nature of the impact. While it is clear the intention is to capture 'malicious' activity, this is not restricted by the current wording of the instrument.

To help understand this, it is important to understand that within a telecommunications network it is possible for third-party events – for example the misconfiguration of a network filter list, or the unintentional abuse of a shared access service – to cause disruption to carrier or carriage service provider's assets. These actions would not normally be classed as a cyber security incident, but based on the proposed wording it would be difficult for a Carrier or CSP to not treat them as such. Additionally, a civil contractor who accidentally severed a communications cable, or a traffic incident that resulted in disruption to the operations of a communications facility would similarly be captured by the instruments' reporting obligations. We consider that unless 'cyber security incident' is more accurately defined, there will be additional burden on carriers/CSPs and that the department will collect large amounts of non-useful data.

Third Party Network Relationships
At present it remains unclear how third-party network relationships should be factored into reporting. While it seems clear that the primary intention is to capture 'tangible' assets, the wording is clearly defined to capture the Virtual network operators as well as physical network operators by including the definitions under section (b) of the definition of an asset.

The obligation to establish control and identify asset components (such as the physical location of the asset and detailed ownership information) is often part of the commercial and confidential nature of a third-party provider in Virtual Operator relationships and is not usually material to the nature of the agreement with a CSP who delivers a 'virtual' telecommunications network. Commercially we anticipate much resistance to us seeking to quantify these assets with our providers and can foresee similar contractual issues with our virtual network clients.

We would suggest that clarification is required to indicate how virtual network relationships should be handled under these rules.

Overly burdensome regulation for smaller operators
We remain concerned that the implementation of these instruments will be overly burdensome for smaller operators, many of whom are sole traders or owner-operator businesses with a small asset base or network footprints. In many cases these operators do not have the operational resources to fulfill the instruments' additional reporting obligations without incurring substantial costs in additional staff and systems resources; which for smaller operators often running incredibly tight margins presents a significant cost of business in relation to their overall operating revenue.

In the consultation briefings, the department indicated that it intended the obligations to consist of some 'safe harbour' provisions to make it clear that such rules would only apply to providers of a certain size. As with other legislative elements, we would propose that a 'Services In Operation' (SIO) threshold would be a good mechanism to indicate whether a provider should be bound by these enhanced reporting obligations, for example providers with less than 25,000 SIOs should not be subject to the instruments.

Lack of definition on method of delivery of asset information
For many modern and agile network providers, asset lists are constantly changing as new networks are built and expanded. In addition, for established networks the tangible and intangible asset list described can be quite large. While the proposed instruments provide a 'general' description of the information required and method of disclosure for reporting, the lack of a specific definition will lead to a number of problems in implementation. Specifically, we are concerned about the substantial cost associated with initially collating and establishing this information, and any subsequent revisions that may need to be taken should a method or format for communicating this to DoHA later be established.

We are also concerned about the method of transmission of such information, and whether any meaningful description of assets would be of any valuable use to any organisation outside of our own due to the varied and specific nature of any such information; unless an appropriate format is defined to document and share this information.

Threshold for asset value and size
We note that there is no current restriction on the requirement of reporting for asset size. Network units – such as residential CPE (Consumer Premises Equipment) devices – would currently fall under the scope of this ruling, and while we note recent public exploit attempts impacting CPE devices, we envisage the department does not intend assets of 'ephemeral' nature, such as these, to be included within the scope of this reporting.

For instance, this would require the disclosure of every residential customer who has a CPE modem that is essential to the provision of their telecommunications service as an 'asset', and to also identify the 'operational control' of this device, disclosing the end user's name, address, and other details as part of this register. While we recognise that such information is already retained by a carriage service provider or carrier under their reporting obligations, this information is protected under appropriate legislative rules, and we do not believe it is appropriate to record this as part of this legislative instrument.

While it was clear from the information sessions and explanatory details that this was not the intention of the proposed rules, the wording does not currently support this reading, and as such the instruments should be amended to clarify the intent of both the size of the asset, and the thresholds for control.

Concerns over protection of data
We note that there are currently no specific protections given to the information being provided to DoHA as part of this reporting obligation within the proposed instruments. Such information is commercially confidential to each entity, and the disclosure or publication of such information is likely to present significant commercial and security risks to an organisation. These details should be specifically protected, and limits on the access to and use of this data should be clearly defined.

We thank you for the opportunity to review these proposed instruments. If you have any questions regarding any aspect of our submission, we encourage you to contact me via email or phone.

Warmest regards,

Andrew Yager
CEO and Director