macquarie
TELECOM GROUP

Submission to the

Review of the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022

24 February 2022

1 Overview

1.1 Macquarie Telecom Group Ltd (**Macquarie**) welcomes this opportunity to contribute to the Parliamentary Joint Committee on Intelligence and Security (**the Committee**) review of the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 (**the Bill**), which amends the *Security of Critical Infrastructure Act 2018* (**the SOCI Act**).

1.2 In short, Macquarie submits that the Bill:

- should not water down the definition of 'critical data storage or processing asset' by excluding those used to store or process government data—that is, data storage or processing service providers that store or process data for Commonwealth and state and territory government entities should be recognised and regulated as critical infrastructure providers;
- should not exempt from the risk management program those data storage or processing service providers that are certified under the Commonwealth's hosting certification framework (**HCF**) until such time as that framework is formalised in the Protective Security Policy Framework;
- should be amended so that the SOCI Act applies extraterritorially to the offshore storage and processing of the business critical data of Australia's critical infrastructure providers; and
- should be amended to give the Minister a power to prevent nationally significant business critical data being stored or processed offshore.

2 About us

2.1 Macquarie is subject to the security of critical infrastructure (**SOCI**) regulatory regime in multiple capacities. We are a licensed carrier under the *Telecommunications Act 1997,* a cloud service provider, and the owner and operator of Australian data centres that store and process the data of Commonwealth and state governments and critical infrastructure providers. Macquarie's data centres are also "certified strategic" under the Commonwealth Government's HCF.

3 Background

3.1 The SOCI Act specifies 11 'critical infrastructure sectors' including the 'data storage or processing sector'[1], which is defined as 'the sector of the Australian economy that involves providing data storage or processing services.'[2]

3.2 The Bill (at section 13) proposes to redefine 'data storage or processing service' as:

> (a) a service that:
> (i) enables end-users to store or back-up data; and
> (ii) is provided on a commercial basis; or
> (b) a data processing service that:
> (i) involves the use of one or more computers; and
> (ii) is provided on a commercial basis; or
> (c) a service that is specified in the rules.

[1] *Security of Critical Infrastructure Act 2018* (**SOCI Act**) s 8D.

[2] SOCI Act s 5.

However, the rules may prescribe that a specified service is not a data storage or processing service.

3.3 The SOCI Act imposes certain obligations of the entities that control the infrastructure assets that are core to each of these 11 sectors.

3.4 An 'asset' is defined as including 'a system, network, facility, computer, computer device, computer program, computer data, premises, or any other thing'.[3]

Critical data storage or processing asset

3.5 An 'asset' constitutes a 'critical data storage or processing asset' if it is 'owned or operated by an entity that is a data storage or processing provider' and either:

3.5.1 is known to be 'used wholly or primarily to provide a data storage or processing service' to a government end-user;[4] or

3.5.2 is known to be 'used wholly or primarily to provide a data storage or processing service that: (i) is provided by the entity on a commercial basis to an end-user that is the responsible entity for a critical infrastructure asset; and (ii) relates to business critical data'.[5]

3.6 The Bill will amend this definition of 'critical data storage or processing asset' in respect of the storage and processing of government data. The existing definition is not concerned with the type of data that is being stored or processed on behalf of a government end-user. However, the Bill will change this so that only those assets used in the storage or processing of 'business critical data' on behalf of a government end-user will be captured.[6]

3.7 'Business critical data' is defined as:

> (a) personal information (within the meaning of the *Privacy Act 1988*) that relates to at least 20,000 individuals; or
>
> (b) information relating to any research and development in relation to a critical infrastructure asset; or
>
> (c) information relating to any systems needed to operate a critical infrastructure asset; or
>
> (d) information needed to operate a critical infrastructure asset; or
>
> (e) information relating to risk management and business continuity (however described) in relation to a critical infrastructure asset.[7]

Responsible entity

3.8 The 'responsible entity' for a critical data storage or processing asset is the entity that owns or operates that asset.[8]

Critical Infrastructure Assets

3.9 A critical data storage or processing asset is a 'critical infrastructure asset'.[9]

[3] SOCI Act s 5.

[4] SOCI Act s 12F(1).

[5] SOCI Act 2 12F(2).

[6] Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 (**SLACIP Bill**) item 32.

[7] SOCI Act s 5.

[8] SOCI Act s 12L(4).

[9] SOCI Act s 9.

3.10 The responsible entity for a critical infrastructure asset must (1) register certain operational information about the asset;[10] and (2) report certain cyber security incidents affecting the asset.[11] Under the Bill, the responsible entity must also adopt and maintain a risk management program, except if the entity has been "certified strategic" by the Digital Transformation Agency under the Commonwealth's HCF, in which case the risk management program requirement does not apply.[12]

3.11 Under the draft Security of Critical Infrastructure (Critical infrastructure risk management program) Rules,[13] a risk management program must address specified 'material risks', including 'an impact resulting from the storage, transmission or processing of sensitive operational information outside Australia'.[14]

Critical Infrastructure Sector Assets

3.12 A critical data or processing asset is also a 'critical infrastructure sector asset'.[15]

3.13 In the event that a cyber security incident has a 'relevant impact' on a critical infrastructure asset, the government has certain powers to direct or provide technical assistance to an responsible entity for, or an owner of, either a critical infrastructure asset or a critical infrastructure sector asset.[16] This reflects the fact that a cyber incident affecting a critical infrastructure sector asset may have a flow on impact to other critical infrastructure assets or providers in the same or another sector.

4 The Bill should not exclude from the SOCI regime those service providers that store and process government data

4.1 As things stand today, a data storage or processing service provider is taken to be a critical infrastructure provider if it supplies a data storage or processing service to a Commonwealth or state and territory entity.[17] The nature of the data concerned is immaterial.

4.2 The proposed amendment in Item 32 of the Bill will change this so that the SOCI Act will no longer apply to such service providers except if the government data they store or process comprises 'business critical data'. This is a significant and dangerous reduction in the scope of the SOCI Act because business critical data does not describe the type of information that is most commonly held by government departments and agencies nor what is crucial to the functioning of government.

4.3 As the name suggests, business critical data reflects the types of information that are crucial to the operation and resilience of commercially run critical infrastructure, not governments. Specifically, business critical data is defined to comprise only:

- personal information;
- R&D information in relation to a critical infrastructure asset;

[10] SOCI Act pt 2. A 'direct interest holder' with an interest in the asset greater than 10% or which otherwise puts it in a position to influence or control the asset must also provide certain 'interest and control information' in relation to the asset.

[11] SOCI Act pt 2B. However, an entity that owns or operates a 'critical infrastructure sector asset' is not required to report cyber security incidents.

[12] SLACIP Bill item 49 new s 30AB(4).

[13] Explanatory Memorandum, SLACIP Bill, Attachment C.

[14] Draft Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (**Draft Rules**) cl 4(c).

[15] SOCI Act ss 8E(1), 8E(3).

[16] SOCI Act pt 3A.

[17] SOCI Act s 12F(1).

- the information or systems needed to operate a critical infrastructure asset; or
- risk management and business continuity information in relation to a critical infrastructure asset.

4.4 As the 2020 Explanatory Memorandum notes, that definition was crafted specifically to reflect the circumstances of commercially run critical infrastructure operations:

> The definition of 'business critical data' outlines the categories of data that are of most significance to the operation and security of 'critical infrastructure assets', or otherwise represent a potential security vulnerability…The purpose of this definition is to limit the application of new subsection 12F(2) of the SOCI Act so that 'critical data storage or processing assets' are those assets owned or operated by a 'data storage or processing provider', and used to store or process 'business critical data' that relates to another asset captured as a 'critical infrastructure asset'.[18]

4.5 Government entities deal in very different types of information to commercially run critical infrastructure operators. However, the security, integrity and accessibility of that government data is no less critical to the continuous functioning of society. Indeed, this was the rationale for originally recognising—and regulating—those that store or process government data as 'critical infrastructure providers'. As noted in the 2020 Explanatory Memorandum:

> Data centres and cloud providers that are custodians of Government data are critical due to [the] sensitive nature of Government information that they store or process. Under the Protective Security Policy Framework, the Australian Government is required to safeguard official information and mitigate the risks of cyber attacks. This is because it is likely that a compromise of Government data may lead to the disclosure of highly sensitive information relevant to the operation of the nation, risk foreign relations with key international partners and undermine economic prosperity and social stability. State and Territory Government also hold sensitive data that is critical to the operation of services and other aspects in their jurisdiction.[19]

4.6 The gaps and consequences arising from the proposed change to the definition are significant and, in the circumstances, seem absurd. For example, a data storage or processing service provider would not be recognised or regulated as a critical infrastructure provider under the SOCI Act if it was storing or processing:

- highly classified government information;
- the entirety of the National Archives of Australia;
- official company records for the Australian Security and Investments Commission or official records of deaths for a state registry office (because 'personal information' within the meaning of the Privacy Act only captures information about natural persons who are still living);
- official geophysical data (e.g. magnetic, seismic and electromagnetic data) and national location information (e.g. Australia's topographic and maritime boundaries) determined by Geoscience Australia or weather telemetry information collected by the Bureau of Meteorology;
- the systems that underpin the operation of the video teleconference links used by the federal and state courts, or the document management and business systems used in the Commonwealth and state and territory parliaments or police stations, or the security

[18] Revised Explanatory Memorandum, Security Legislation Amendment (Critical Infrastructure) Bill 2021, para 62–3.
[19] Ibid, para 369.

controls and surveillance systems used in prisons (as courts, parliaments, police stations and prisons are not considered 'critical infrastructure assets' in their own right).

4.7 The data storage or processing service provider in these scenarios would not be required to do anything under the SOCI Act—not even report a cyber-attack on its (or its suppliers) systems that potentially or actually affected the integrity or availability of the government data.

4.8 The reason for the proposed amendment is not obvious and is not explained. It may be that the government's HCF is considered an adequate alternative to regulation under the SOCI Act. Indeed, the Bill (at Item 49 in new subsection 30AB(4)) proposes to exempt data storage or processing service providers from the risk management program requirements if they hold a so called "strategic" certification under the HCF. However, the HCF is not equivalent to the SOCI regime and is at best only a partial substitute to the SOCI Act given that the HCF:

- is not grounded or specified in any legislation or formal regulatory instrument;
- does not apply to data storage or processing for corporate Commonwealth entities or state and territory government entities;[20]
- does not require any reporting of cyber incidents (like Part 2B of SOCI Act); and
- does not provide for government (ASD) intervention and technical assistance in the event of a major cyber security incident (like Part 3A of the SOCI Act).

4.9 Moreover, any reliance on the HCF in lieu of regulation under the SOCI Act may lead to those service providers that store or process government data being overlooked and excluded as, over time, other Commonwealth and state/territory laws attach new responsibilities and obligations on "official critical infrastructure providers" (e.g. in disaster planning, or when designating essential industries or workers, or rationing access to liquid fuel during national emergencies).

4.10 The proposed amendment in Item 32 of the Bill should not proceed. A data storage or processing service provider that stores or processes any form of government data should absolutely be recognised and regulated as a critical infrastructure provider. If the proposed amendment does proceed, then the definition of business critical data in section 5 of the SOCI Act must be broadened to reflect the types of sensitive and classified information that are commonly held by Commonwealth and state and territory government entities. At a minimum, that should include all security classified information and all operational data and systems of emergency service organisations.

5 The method and timing of the exemption of service providers certified under the HCF should be reconsidered

5.1 Item 49 of the Bill proposes to insert a new subsection 30AB(4) that would exempt data storage or processing service providers from the risk management program requirements in Part 2A if the provider holds a so called "strategic" certification under the HCF (**the HCF exemption**). An exempted service provider would still have to report annually to the Secretary of Home Affairs on the effectiveness of its risk management.[21]

5.2 It is reasonable to exempt such service providers from Part 2A given the HCF involves a similar risk management process. However, this should not be done through primary legislation until the HCF is itself formalised in legislation or regulation or at least incorporated into the Protective Security Policy Framework. This seems unlikely to occur before the enactment of the Bill but new

[20] Such as those described in section 12F(1)(b) of the SOCI Act.

[21] SLACIP Bill, item 49 new s 30AQ.

subsections 30AB(5)–(6) provide the means for the HCF exemption to be achieved at a later time via a subordinate instrument.

5.3 The Committee should note that the HCF exemption would have some drawbacks. In particular, a service provider certified under the HCF would not be required to address any of the 'material risks' that the Minister may specify for the purposes of new subsection 30AH(8). These are set out in the draft Security of Critical Infrastructure (Critical infrastructure risk management program) Rules 2022 (**the draft Rules**), which has been published as Attachment C to the Explanatory Memorandum to the Bill. Although many of the specified material risks are reflected in the HCF,[22] there are some that are not, such as risks associated with 'the storage, transmission or processing of sensitive operational information outside Australia'.[23]

5.4 Ideally, all critical data storage or processing service providers should be asked to minimise or eliminate an equivalent set of risks—to the extent they are relevant—whether they are certified under the HCF or regulated under Part 2A of the SOCI Act. Those service providers all face similar hazards and must address similar risks no matter which scheme regulates their risk management practices.

6 The SOCI Act should apply extraterritorially to business critical data stored and processed offshore

6.1 The SOCI Act—since its original enactment in 2018—applies extraterritorially.[24] As the accompanying Explanatory Memorandum noted at the time:

> In order for Australia to exercise jurisdiction, such as regulating certain conduct, in relation to matters or actions occurring outside of Australia, it must also have a basis for doing so under international law. This requires a sufficient degree of connection to Australia, which, for example, in respect of foreign operators of critical infrastructure assets with[in] Australia, this nexus would be met. Further, if there was an example of a foreign entity engaging in conduct overseas, but where the conduct affects the security of Australia, this would also provide a sufficient degree of connection to Australia.[25]

6.2 The 2021 amendments to the SOCI Act sought to define new critical infrastructure sectors by reference to assets that are located in Australia. Specifically, subsection 9(2B) of the SOCI Act states that 'An asset is not a critical infrastructure asset if, or to the extent to which, the asset is located outside Australia'.

6.3 This approach is problematic in a digital context, a fact that was noted in the Committee's Report:

> [S]ome definitions capture all assets within a broad sector, such as the definition of a critical data storage or processing asset in proposed section 12F, but then identify that some specific assets may not be an asset as defined, if precluded in the rules. This particular asset definition also does not seemingly recognise potential extraterritorial impact of the broad coverage of this definition, as affected providers may operate within Australia on relevant data held within Australia, but may hold part of that data offshore, or shift it offshore or have primary operations (including data centre assets) in other countries. This is in contrast to many of the other assets that relate to physical assets bound to Australian territory and operation within the country.

[22] See Digital Transformation Authority, *Whole of Government Hosting Strategy Hosting Certification Framework*, March 2021, p 19 Table 7.

[23] Draft Rules cl 4(e).

[24] SOCI Act s 14.

[25] Revised Explanatory Memorandum, Security of Critical Infrastructure Bill 2017, p 40 para 217.

> The application of asset definitions only to assets that are located within Australia (as per proposed subsection 9(2B)), further confuses the potential application to digital elements of critical infrastructure entities that have parts of their functional infrastructure or data located offshore, as mentioned above.[26]

6.4 The Bill does not address this issue of extraterritoriality. Consequently, although the SOCI Act is intended to apply extraterritorially where there a link between the conduct occurring overseas and the security of Australia's critical infrastructure, it does not apply to data storage or processing assets that are outside Australia but nonetheless 'wholly or primarily' being used to store or process business critical data of Australian critical infrastructure providers. That is, the SOCI Act does not apply to data storage or processing service providers in Australia that are storing and processing Australian data overseas.

6.5 Accordingly, such service providers are not required to register ownership and operational information in respect of those offshore assets as others must under Part 2 of the SOCI Act. Nor are they required to report cyber security incidents that affect those offshore assets as others must under Part 2B. They would not have to adopt and maintain a risk management program as others must under the Bill. And the government will have no powers under Part 3A to direct or provide technical assistance to those service providers in the event a serious cyber incident affects those offshore assets, notwithstanding the potential direct impact such incidents might have for operation of critical infrastructure assets in Australia.

6.6 Further, the Minister is prevented from *ever* bringing into the SOCI regime a data storage or processing asset that is located overseas, no matter how critical it may be to the functioning of Australia's economy or society.[27] Although the Minister may, under subsection 9(1)(f) and section 51 of the SOCI Act, declare a particular asset to be a 'critical infrastructure asset', those powers can only be used in respect of an asset that is located in Australia.

6.7 This jurisdictional gap creates a perverse incentive for all types of critical infrastructure providers—and their suppliers—to shift data stores and processing functions offshore where they will be beyond the scope of the SOCI Act and can avoid the associated security requirements and compliance costs. If all business critical data was shifted offshore then the SOCI Act would be meaningless in today's digital world.

6.8 It also puts those data storage and processing service providers whose relevant assets are based entirely in Australia at a competitive disadvantage relative to those whose assets are located overseas. Generally speaking, the former will tend to be Australian companies and the latter will tend to be foreign multinational corporations. Such an outcome presumably was not the intention of the 2021 amendments. As the Explanatory Memorandum notes:

> This framework will apply to owners and operators of critical infrastructure regardless of ownership arrangements. This creates an even playing field for owners and operators of critical infrastructure and maintains Australia's existing open investment settings, ensuring that businesses who apply security measures are not at a commercial disadvantage.[28]

6.9 The rationale for excluding critical Australian data storage and processing assets located overseas has not been explained. It is in stark contrast to the approach adopted in other laws, which expressly apply to data stored overseas. For example, the Privacy Act,[29] the Consumer Data

[26] Parliamentary Joint Committee on Intelligence and Security, *Advisory report on the Security Legislation Amendment (Critical Infrastructure) Bill 2020 and Statutory Review of the Security of Critical Infrastructure Act 2018,* September 2021, p 22–3 para 2.51–2.52.

[27] See, e.g., SOCI Act ss 9(1)(f), 51.

[28] Explanatory Memorandum, Security Legislation Amendment (Critical Infrastructure) Bill 2020, para 9.

[29] *Privacy Act 1988* (**Privacy Act**) s 5B.

Right,[30] the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*,[31] and the Data Availability and Transparency Bill 2020, which is currently before Parliament.[32] Indeed, the Explanatory Memorandum to the Data Availability and Transparency Bill succinctly explains why extraterritorial application is necessary for Australian laws intended to govern the use or security of Australian data assets:

> Establishing extraterritorial application of this Bill is necessary given foreign entities may be accredited, and technological advances mean that data is increasingly stored offshore and may be accessed remotely. Extending the application of the Bill in this way ensures the data sharing scheme's safeguards apply consistently to all participants and situations, and are capable of adapting to emerging and future needs. Consistent with relevant schemes such as the Privacy Act and the Criminal Code, subclause (1) and clause 136 provide that the Bill and applicable sections of the Regulatory Powers Act have extraterritorial effect.[33]

6.10 Similarly, the SOCI Act should apply consistently to all participants and situations involved in the storage and processing of the business critical data of Australia's critical infrastructure providers, regardless of whether that storage and processing is undertaken here or overseas.

6.11 This could be achieved by amending the Bill so that it deletes existing subsection 9(2B) of the SOCI Act and replaces it with a new subsection 9(2B) that says:

> An asset is not a critical infrastructure asset if, or to the extent to which, the asset is located outside Australia, unless the asset is a critical data storage or processing asset, in which case this subsection 2B does not apply to that asset.

6.12 This may warrant a consequential amendment to broaden the definition of the 'responsible entity' in relation to a critical data storage or processing asset that is located outside of Australia, which can be done through subordinate rules under subsection 12L(4)(c) of the SOCI Act.[34] This could mimic the so called accountability approach reflected in Australian Privacy Principle (**AAP**) 8.1, whereby the 'AAP entity' that intends to disclose personal information to an overseas recipient is required to take reasonable steps to ensure that the recipient does not breach the APPs in relation to the information.[35] That usually requires the APP entity to impose contractual obligations on the recipient. The APP entity remains accountable for acts or practices done by the overseas recipient.[36]

6.13 It is not unreasonable to expect that a data storage or processing service provider will take reasonable steps to ensure that any overseas facilities it plans to use to store or process the business critical data of an Australian critical infrastructure provider will meet the minimum security requirements under the SOCI Act—especially if the parties involved are related companies in the same corporate group. Indeed, the draft Rules specifically set security benchmarks by reference to foreign and international standards to 'provide industry with the necessary flexibility to comply with their statutory obligations by recognising alternative cyber security frameworks that achieve the desired uplift in security and resilience…'.[37]

---

[30] *Competition and Consumer Act 2010*, s 56AO.

[31] See, e.g., *Surveillance Devices Act 2004*, pt 5 which provides for the extraterritorial operation of computer access warrants and data disruption warrants.

[32] Data Availability and Transparency Bill 2020, ss 7, 136

[33] Explanatory Memorandum, Data Availability and Transparency Bill 2020, para 17–18.

[34] SOCI Act s 12L(4).

[35] Privacy Act AAP 8.1.

[36] Privacy Act s 16C.

[37] Draft Explanatory Statement, Draft Security of Critical Infrastructure (Critical infrastructure risk management program) Rules, p 18.

6.14 If extraterritorial application happened to present an intractable problem in a particular case, the SOCI Act already provides the means for the Minister to exclude a specified critical data storage or processing asset.[38]

6.15 The SOCI Act will not help secure Australia's critical data and will become digitally irrelevant if it is not applied consistently to critical data storage and processing assets, wherever they may be located. It would be far better to ensure that all such relevant assets are within the scope of the SOCI Act even if some of them subsequently have to be excluded through regulation. To do otherwise is to surrender Australia's sovereignty over its critical data assets when it has never mattered more.

7 The Bill should give the Minister a power to prevent nationally significant business critical data being transferred offshore

7.1 The SOCI Act is deficient in that it does not provide any mechanism to protect nationally significant critical data workloads from being transferred and run offshore, potentially outside Australia's jurisdiction.[39] The Bill does not address this aspect at all.

7.2 This is a serious omission. Such a safeguard will become increasingly important to the cyber resilience of Australia's critical infrastructure as operational technologies (**OT**)—i.e. the networks of devices and software that control industrial operations and processes—are increasingly connected to and converged with information technology (**IT**)—i.e. the data processing infrastructure—and shifted into a cloud computing environment.

7.3 As a precautionary measure and to future-proof the SOCI regime from the rapid pace of technological change, the Bill should be amended to give the Minister a power to declare particular business critical data to be of national significance and thereby prevent it from being stored or processed outside of Australia if such an outcome would not be in the national interest.

7.4 The Parliament has effectively already declared MyHealth records and the National COVIDsafe Data Store as falling within such a category and prohibited such data being stored or processed outside of Australia.[40] And the Committee reached a similar conclusion about telecommunications metadata, recommending in October 2020 that such information be required by law to be stored 'on servers located in Australia unless specifically exempted'.[41]

7.5 It is easy to foresee other potential scenarios in the coming decade where it might be necessary or desirable for the government to promote the digital resilience of particular critical infrastructure assets by imposing similar restrictions on the international transfer of other critical data workloads. By way of example, this conceivably could include:

- the supervisory control and data acquisition (**SCADA**) systems that control Snowy Hydro's mechanical plant or which manage the rail traffic signalling and track switching on the Australian Rail Track Corporation's rail network;
- the clearing and settlement systems and central securities depositories that underpin the operations of the Australian Securities Exchange (**ASX**);

[38] SOCI Act s 9(2).

[39] Although section 32 of the SOCI provides for the Minister to direct a critical infrastructure provider to do, or refrain from doing, a specified act or thing if there is risk to security, that power is limited to circumstances where ASIO has made an adverse security assessment in respect of the provider. That is different to the type of scenario envisaged in this submission.

[40] See *My Health Records Act 2012* s 77 and Privacy Act s 94F.

[41] Parliamentary Joint Committee on Intelligence and Security, *Review of the Mandatory Data Retention Regime*, October 2020, recommendation 21.

- the inventory or logistics management systems used by private sector participants involved in the management of Defence assets, the National Medical Stockpile or similar national resources;
- automated remote patient monitoring platforms used in public hospitals; or
- certain non-active data sets, such as the blueprints or schematics of key institutions (e.g Parliament House) or infrastructure (e.g. the East Coast gas grid) or bathymetry survey data that maps the topography of the Australian sea-floor.

7.6 This new Ministerial power would align with the Treasurer's existing power and recent practice under the *Foreign Acquisitions and Takeovers Act 1975* to impose data conditions on foreign takeovers.[42] Ironically, as things stand today, a critical infrastructure provider can be prevented from shifting critical data offshore if a foreign investor acquires a controlling stake in the business but not if the business remains Australian owned. Clearly, the arrival of a foreign investor is not the main cause of data storage and processing functions being shifted offshore—as noted above, the SOCI Act itself creates an incentive to do so.

7.7 This recommendation could be achieved by amending the Bill to insert a new Part 6B in the SOCI Act dealing with the 'Declaration of business critical data of national significance by the Minister'. This could replicate the consultation and notification provisions of the new Part 6A (regarding the Declaration of systems of national significance by the Minister) and provide that any business critical data that is declared to be of national significance must not be stored, transferred or accessed outside Australia. The test for national significance could take account of such factors as:

- the nature and extent of any interdependencies between particular business critical data and one or more other critical infrastructure assets;
- the consequences that would arise for the social or economic stability of Australia or its people, or the defence of Australia, or national security if a hazard were to occur that had a significant relevant impact on the business critical data in question; and
- the potential to minimise or eliminate the material risk of such a hazard occurring by keeping the storage, transmission or processing of the particular business critical data in Australia.

-END-

[42] Foreign Acquisitions and Takeovers Act 1975 s 74(2). See also Glenda Korporaal, 'Protect data in foreign takeovers: FIRB chief', *The Australian* (online, 21 August 2019). The Government is also 'considering whether certain data sets [held by government] of concern to the public should be declared sovereign data sets and should only be hosted in Australia, in an accredited Australian data centre, across Australian networks and only accessed by the Australian government and our Australian service providers', see Stuart Robert MP, 'Government services in the digital age: the challenges, the plan and the delivery' (Speech, National Press Club, 7 July 2020).