27 November 2020

Department of Home Affairs
Submitted via online form

Subject: Submission in response to the Exposure Draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020

Dear Sir/Madam,

Please find enclosed the .au Domain Administration Limited's (auDA) submission in response to the Exposure Draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020.

Our submission focuses on the following key issues:

- **Definitional Issues**
- **Rule-making power**
- **Positive Security Obligations**
- **Enhanced Security Obligations**
- **Government Assistance**
- **Self-Incrimination and self-exposure**

Who is auDA?

The .au Domain Administration Ltd (auDA) is a not-for-profit company limited by guarantee that oversees the operation and management of the .au domain of the Internet.

auDA is endorsed by the Commonwealth Government as the appropriate entity to administer Australia's country code Top-Level Domain (ccTLD) - the .au domain - on behalf of Australian Internet users. The International Corporation for the Assignment of Names and Numbers (ICANN) delegated management of the .au ccTLD to auDA in October 2001 through a *Sponsorship Agreement* which requires auDA to ensure the stable and secure operation of nameservers.

The Commonwealth Government has reserve powers over electronic addressing in the *Telecommunications Act 1997* and the Australian Communications and Media Authority Act 2005 to provide for intervention in the event that auDA was unable to manage electronic addressing in an effective manner.

What do we do?

The .au domain plays an important role in supporting the digital economy with over 3.2 million domain names registered as at August 2020.

auDA's core task is to ensure the ongoing availability of .au domain names to support business, information and email services for Internet users.

The Domain Name System (DNS) enables internet users to find websites by using domain names rather than needing to remember a series of numbers (IP addresses). auDA maintains the database of domain names within .au and manages the .au domain name service. auDA uses contracts with the Registry and Registrars to deliver this service.

What is our relationship with government?

In October 2017, the Minister for Communications announced a review of Australia's management of the .au domain. The review concluded reforms were needed for the company to continue to perform effectively and meet the needs of Australia's Internet community. The review reflected three principles:

- the Australian Government is committed to strengthening multi-Stakeholder mechanisms for internet governance given the Internet is a collection of distributed and transnational networks and its governance is an international issue;
- the .au namespace is a public asset and should be governed with community interests in mind; and
- auDA has a monopoly position and should be subject to stringent oversight requirements.

The review acknowledged that auDA has introduced many important policy and security initiatives and that .au is seen globally as a secure and trusted namespace.

The review identified auDA as Critical Infrastructure given "disruption to critical infrastructure could have a range of serious implications for business, government and the community."

The importance of security of the Domain Name System was an area of focus in the review. The review considered that maximising the security and technical stability of the .au domain space remained an appropriate articulation of auDA's role in the immediate future.

auDA accepted and implemented all the recommendations of the review with a final letter from the Minister for Communications on 25 May 2020 acknowledging auDA's successful completion of the reforms.

auDA's focus on Security of the DNS

auDA's company constitution makes specific reference to on the *Objects* clause to "maintain and promote the operational stability and utility of the .au ccTLD and more generally the Internet's unique identifier system, and to enhance the benefits of the Internet to the wider community.

auDA's *Terms of Endorsement* include core functions of "ensure stable, secure and reliable operation of the .au domain space" and "respond quickly to matters that compromise DNS security" and specific conditions that auDA engage with the Commonwealth Government and support trust and confidence in .au through a range of security-focused measures including an enterprise security strategy informed by domestic and international best practice. As required by the review, there is a public-facing version of the Enterprise Security Strategy on auDA's website.

auDA has recently updated the *Policy Framework* for .au through new *Licensing and Registrar Rules* and a new *Registrar Agreement*. auDA is in the process of implementing these new arrangements and the new agreement. The new agreement has obligations for enhanced security standards and a power for auDA to suspend accreditation until the agreed standard has been met.

The review of auDA recommended auDA engage with Commonwealth Government security agencies. auDA has built strong relationships with Australian Signals Directorate, Australian Cyber Security Centre, the Critical Infrastructure Centre and in particular the

Communications Sector Group within the Trusted Information Sharing Network (TISN). The Department of Communications and the Arts has a role in facilitating partnerships between auDA and relevant cybersecurity agencies.

auDA reports quarterly on its activities, including security-related, for example, progress towards ISO 27001 accreditation and achievement of the accreditation.

The review of auDA recommended that auDA engage with key international security fora including ICANN's Security and Stability Advisory Committee to ensure auDA is kept undated on international security developments. auDA has been participating actively in ICANN over many years and through 2020 in remote conferences.

Internally, auDA's Board has established a Security and Risk Committee to focus on internal controls, privacy, security management, risk management and business continuity.

For questions relating to this submission, please contact Caroline Fritsch, [redacted].

Yours sincerely,

[redacted]

Rosemary Sinclair AM
CEO
.au Domain Administration Ltd

November 2020

auDA Submission

Home Affairs
Security Legislation Amendment
Critical Infrastructure Bill 2020

1. .au Domain Administration Limited (auDA) welcomes the opportunity to make a submission in response to the Exposure Draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 ('the Bill'). auDA previously made a submission and supplementary submission to the Department of Home Affairs ('the Department') *Protecting systems of national significance and critical infrastructure* consultation paper (September 2020). auDA refers the Department to its earlier submission to provide essential background and context for its commentary in this submission.

2. auDA acknowledges the Department's genuine willingness to engage with it on the consultation paper and Bill, but remains concerned that the three week consultation window for the Bill is too short to understand the complexity of the provisions and assess the technical and operational feasibility of complying with obligations. auDA also believes comprehension of the Bill is frustrated by the absence of draft rules and approved forms, which contain the substantive detail of some of the obligations. As a result, this submission focuses on a few high-level concerns and does not attempt to address issues relating to the Enhanced Security Obligations, and Government assistance. auDA would welcome an opportunity to provide a supplementary submission on these issues.

3. All references to sections in this submission relate to the Bill, unless otherwise indicated.

ISSUES

Definitional Issues

Australian domain name system

4. The definition of communications sector under clause 7 of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 ('the Bill') includes the term 'Australian domain name system.' The Bill does not define the term. However, the Explanatory Document implies that the Australian domain name system 'refers specifically to the .au namespace.'[1]

[1] Explanatory Document, Security Legislation Amendment (Critical Infrastructure) Bill 2020, 11[53]

5. auDA believes that the term 'Australian domain name system' is ambiguous and may be interpreted as including other domains that have an Australian nexus.[2] Australia has five country code Top Level Domains (ccTLDs) assigned to it, which are based on the country code ISO 3166-1 alpha 2:

    a) .au ccTLD - Australia

    b) .cc ccTLD - Cocos (Keeling) Islands

    c) .cx ccTLD - Christmas Island

    d) .nf ccTLD - Norfolk Island

    e) .hm ccTLD - Heard Island.

6. There are also two generic Top Level Domains (gTLDs) assigned to Australian States on the basis of geo-political units:

    a) .sydney gTLD - State of New South Wales

    b) .melbourne gTLD - State of Victoria

7. While the .au ccTLD is the largest Australian domain and essential to the functioning of the Australian economy, government and society, auDA notes that a cyber security incident may have a significant impact on other Australian ccTLDs, especially where government, businesses and essential services rely on that domain to provide services to communities residing in an external Territory, such as the Norfolk Island Regional Council http://www.norfolkisland.gov.nf/.

8. auDA recommends that the term Australian domain name system be clarified by reference to either the .au ccTLD, or one or more Australian ccTLDs and gTLDs.

National Security

9. Section 5 of the *Security of Critical Infrastructure Act 2018* (Cth) ('the SOCI Act') defines national security as meaning "Australia's defence, security or international relations." This definition is pivotal to the exercise of powers under the Bill, including:

---

[2] Clause 7 of the Bill defines Australia "when used in a geographical sense, including the external Territories." Also see *Security of Critical infrastructure Act 2018* (Cth), s13.

a) prescribing by the rules or declaring that an asset is a critical infrastructure asset
b) information gathering directions
c) action directions
d) intervention requests

10. National security considerations have also been used to justify exempting Ministerial authorisations under Part 3A of the Bill from review under the *Administrative Decisions Judicial Review Act 1977* (Cth).[3]

11. auDA believes that the scope of the definition is unclear and potentially very wide, especially given the intrusive nature of the proposed powers and penalties under the Bill. auDA strongly contends that any definition of national security should be explicit as to the activities, conduct and interests that are caught. This provides an important safeguard as to the scope of the Ministerial authorisation power, and also goes to the question of jurisdictional error for the purpose of seeking a remedy associated with judicial review of a Ministerial authorisation under the original jurisdiction of the High Court and Federal Court of Australia.

12. auDA advocates for a more comprehensive definition of national security, such as the definition of national security under section 90.4 of the *Criminal Code Act 1995* (Cth) with the scope of the definition limited to the national security of Australia. However, if the current definition of national security is retained, auDA considers that the key terms 'defence', 'security' and 'international relations' should be defined. auDA notes that section 5 of the SOCI Act already includes a definition of security, which incorporates by reference the security definition under section 4 of the *Australian Security Intelligence Organisation Act 1979 (Cth).* This definition is attractive as it sets out in concrete terms the security activities and interests that the SOCI Act and Bill are designed to protect.

13. auDA is also attracted to the definition of international relations under section 10 of the *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth), which defines 'international relations' to mean 'political, military and economic relations with foreign governments and international organisations.' This

[3] Explanatory Document, Security Legislation Amendment (Critical Infrastructure) Bill 2020, 65[416]-[422]

definition would accommodate and be consistent with Australia's statements that it will comply with the United Nations Norms of Responsible State Behaviour in Cyberspace, including the requirement to prevent misuse of Information Communication Technology (ICTs) in its Territory and to protect Critical Infrastructure,[4] as well as Australia's existing 'five eyes' arrangements.

Imminent

14. The term imminent is used as threshold criteria to trigger the obligation for a responsible entity to notify the Australian Signals Directorate (ASD) of a cyber security incident[5] and the Ministerial authorisation power for government action to prevent a serious cyber security incident.[6] auDA notes that the term 'imminent threat' is used as an exception to the requirement to consult under 30AL on the making of rules dealing with a critical infrastructure risk management programs. auDA addresses this issue later in this submission.

15. The Bill does not define the term 'imminent' so it should be given its ordinary or dictionary meaning. The Australian Oxford English Dictionary defines imminent in respect of an event as 'impending or about to happen.' This definition creates two temporal standards for when a cyber security incident may be 'imminent':

    a) about to happen implies an immediacy (within hours) as to when the cyber security incident will be launched, such as when a person is about click the button that executes already written code.
    b) Impending implies an elongated time frame and may include preparatory activities for the launch of a cyber-attack or incident in the future.

16. The Tallinn Manual 2.0 International Group of Experts (IGE) considered this issue in the context of cyber operations and the right to anticipatory self-defence. The majority of the IGE considered that the traditional interpretation of imminence

[4] Commonwealth of Australia, Department of Foreign Affairs and Trade, International Security and Cyber Space at the UN (https://www.dfat.gov.au/international-relations/themes/cyber-affairs/international-security-and-cyberspace).
[5] Security Legislation Amendment (Critical Infrastructure) Bill 2020, 530BD
[6] Ibid, s3AB, s12P

which permits a State to only act in anticipatory self-defence where the necessity to act is "instant, over-whelming, leaving no choice of means, and no moment of deliberation" was inappropriate in the context of cyber operations.[7] A State would be required to act immediately before an adversary would be about to press the button that launches the cyber-attack. Given the immediacy and fast paced nature of cyber operations once executed, the State would be deprived of any opportunity to prevent or take action to stop the cyber operation.

17. The majority of the IGE preferred the standard of the "last feasible window of opportunity' to act in anticipatory self-defence.[8] The IGE recognised that this 'window may present itself immediately before the attack, or in some cases long before it occurs' and may be open to abuse and interpretation. However, the critical issue is not the temporal proximity of the action to the cyber incident or attack, but whether a failure to act at that moment, would reasonably be expected to result in the Government being unable to defend itself or stop the cyber operation.[9] Australia has supported a variation of this standard in its Position on the Application of International Law on State Conduct in Cyber Space.[10]

18. auDA believes that the 'last feasible window of opportunity' standard should be applied to the use of government powers under Part 3A to prevent an imminent and serious cyber incident from occurring. This provides an important safeguard that these powers will only be used in an emergency situation, where failure to act in that 'window' will deprive the entity and Government of the ability to take action to prevent the impact of the incident on the asset. auDA notes that where an imminent cyber security incident has not entered the 'window of last opportunity' that the Government should be required to use its other legislative powers to disrupt or prevent the incident. auDA recommends that the Explanatory Memorandum clarify the standard to be applied.

---

[7] International Group of Experts, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd Edition, Cambridge University Press 2017) 350

[8] Ibid 351.

[9] Ibid 351

[10] Australian Government, Department of Foreign Affairs, Annex A: Supplement to Australia's Position on the application of International Law to State Conduct in Cyberspace (accessed 25 November 2020) https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/2019_international_law_supplement.html

19. auDA acknowledges that the 'last feasible window of opportunity' may not be an appropriate standard to apply to the requirement to notify ASD of an imminent cyber security incident under section 30BD(1). However, auDA does not believe that applying another standard will resolve the problems with the practical operation of this obligation. The Explanatory Guide provides the following guidance on the operation of this provision "this may include incidents such as compromises of a computer system where the malicious actor is yet to interfere with the operation of the asset, data theft and exfiltration, or persistent targeting or attempted access to a network where the entity believes a compromise is imminent." [11] This would require a reporting entity to estimate the following likelihoods based on incomplete information:

    a) the likelihood that a range of ad hoc incidents are indicator of or a precursor to the launch of a cyber security incident
    b) likelihood that the cyber security incident is imminent (impending or about to happen)
    c) likelihood that the cyber security incident is likely to have a relevant impact on an asset

20. It is unclear at what stage an entity becomes aware that a cyber security incident is imminent. This is particularly problematic given that failure to comply with this obligation may attract a civil penalty of 50 penalty units and trigger the use of monitoring powers under Part 2 of the Regulatory Powers (Standard Provisions) Act 2014 ('the Regulatory Powers Act'). auDA acknowledges that in very limited circumstances that an entity may become aware of an imminent cyber security incident, such as where malware has infected other critical infrastructure assets on which an asset is dependent and spreading rapidly. auDA recommends that the Department revisit the feasibility of this provision as currently drafted.

Rule-making power

21. The Bill is heavily reliant on the rule making power under section 61 of the SOCI Act to provide the substantive detail of the obligations, and the critical infrastructure assets to which they will apply. This makes it difficult for auDA to

[11] Explanatory Document, Security Legislation Amendment (Critical Infrastructure) Bill 2020, 50[322]

identify and assess the full impact of the proposed legislation on auDA, the registry operator and auDA accredited registrars. As such, auDA believes that genuine consultation with industry will be required to ensure that the Rules are a necessary and proportionate response and consistent with the objects of the SOCI Act.

22. auDA welcomes the following statement in the Explanatory Document that "all rules will be developed through extensive consultations, across industry and Government and will outline expectations and what would be considered a reasonable and proportionate response to meeting the obligations."[12] auDA notes that there is an explicit statutory consultation requirement under section 30AL, which provides for a 14 day consultation period for draft rules relating to critical infrastructure risk management programs (s30AH) by posting the rules on the Department's website. However, the Minister may dispense with the obligation to consult where there is an imminent threat that a hazard will have, or a hazard is having or has had a significant relevant impact on the CI asset.

23. In relation to the statutory consultation requirement under section 30AL, auDA expresses the following concerns:

a) the consultation process relies on an entity monitoring the Department's website as there is no positive obligation for the Minister to notify entities that may be affected by the rules
b) consultation is too short and does not take into consideration the time required for an entity to consider the impact on its operations, including implementation and resourcing issues and to consult with the appropriate senior management or Board committees
c) there are significant penalties for failure to have, comply and update a critical infrastructure risk management program, and failure to meet these obligations may result in the exercise of monitoring powers under Part 2 of the *Regulatory Powers Act 2014* (Cth).

24. auDA notes that the Minister may waive this consultation requirement where he or she is satisfied that there is an imminent threat that a hazard is likely to have a

[12] Explanatory Document, Security Legislation Amendment (Critical Infrastructure) Bill 2020, 47[298]

significant relevant impact on a critical infrastructure hazard. auDA questions the appropriateness of using the critical infrastructure risk management program provisions and associated rule making power as mechanism to deal with imminent threats.

25. All other rules made under section 61 of the SOCI Act are subject to the default consultation requirements under section 17 of the *Legislation Act 2003* (Cth). This requires that before making the rules, the Minister must be satisfied that appropriate consultation, as is reasonably practicable, has been undertaken. This includes consultations with persons who have expertise in the relevant fields[13] and persons that are likely to be affected by the rule.[14] auDA does not believe that this statutory consultation requirement is adequate for the development of rules that are technically complex and will have a significant impact on the operations of an entity.

26. auDA strongly recommends the inclusion of a specific statutory consultation requirement in the Bill that:

a) sets a minimum consultation period of 30 days before any rule can be made
b) requires the Department to notify all responsible entities entered on the Register of Critical Infrastructure Assets, critical infrastructure asset operators (where they do not appear on the Register) and any party that is likely to be affected by the rules
c) the Minister to must take into consideration any financial costs that will be incurred by the entity in meetings its obligations

27. auDA believes that it is important that any rules take into consideration the different sub-sectors within a critical infrastructure sector, and that the rules do not adopt a 'one-size fits all approach.' auDA is committed to working with the Department to co-design the sector specific rules for the communications sector and more specifically the sector for the .au domain name system.

Positive Security Obligations

[13] *Legislation Act 2003* (Cth), s17(2)(a)
[14] Ibid, s17(2)(b)

28. auDA welcomes the Australian Government's proposal that the Positive Security Obligations (PSOs) will not be switched on for auDA, the Registry Operator and auDA accredited registrars due to the current governance and oversight mechanisms for this subsector.[15] As this proposal is conditional, auDA strongly recommends that the Government consult with the sector before 'switching on' the PSOs for one or more critical infrastructure assets.

Critical infrastructure risk management plans

Exception to requirement to consult

29. auDA reiterates its earlier concerns about the rule making power in respect of critical infrastructure risk management programs being used to deal with imminent threats to critical infrastructure assets. [16] auDA believes that it is an inappropriate and probably ineffective mechanism to deal with imminent threats as reporting entities will need sufficient time to assess the potential impact on their asset, identify the most appropriate risk mitigation strategy, update their plan, have the plan approved by the appropriate risk management committee or person, and then implement that plan. auDA believes that if there is an imminent threat that requires changes to critical infrastructure risk management plans, that consultation is critical for entities and Government to fully understand the nature of the threat, the types of harms that may eventuate, and potential risk mitigation strategies. This is particularly important given that Government may "mandate the steps that responsible entities should be taking through their risk management program to address these risks, including in relation to governance arrangements."[17]

30. The exception to the consultation requirement under the proposed new section 30AL, also allows the Minister to dispense with consultation where a hazard has occurred or is occurring. auDA is unclear as to why the Minister would need to dispense with consultation in these circumstances, especially as the entities that have dealt with or are dealing with the hazard may be able to share 'lessons learned' and what risk mitigation strategies may be effective and appropriate given their experiences.

[1515] Explanatory Document, Security Legislation Amendment (Critical Infrastructure) Bill 2020, 14[74]

[16] Security Legislation Amendment (Critical Infrastructure) Bill 2020, s30AL(3)

[17] Explanatory Document, Security Legislation Amendment (Critical Infrastructure) Bill 2020, 47[294]

31. auDA acknowledges that there is a review mechanism where the rules have been made without consultation, however, notes that the 60 day window for the completion of the review from the date the rules were made or amended does not address the immediate regulatory impost placed on entities to update and comply with their critical infrastructure risk management plan when the rules are made.

Annual report

32. Section 30AG requires that a responsible entity must provide an annual report to the Secretary (or other Commonwealth regulator) on its compliance with its obligations under Part 2A by 30 July each year. It is difficult to assess the regulatory burden of complying with this obligation and whether the requirement to report by 30 July is reasonable given:

a) that the approved form is not available to assess the level and detail of information that must be provided[18]
b) that the further guidance material to support the obligation is not available[19]
c) that the annual report must be signed by each Director of the auDA Board.[20]

Failure to comply with the annual reporting requirements attracts a civil penalty of 200 penalty units ($44,400). Given these issues, auDA strongly recommends that the deadline for providing the annual report be moved from 30 July to 1 October (91 days) to give entities sufficient time to prepare the report and get appropriate sign off.

33. auDA questions the requirement for the annual report to be signed by each director of its Board. The Explanatory Document states that certification of the annual report by all directors "is designed to ensure that the most senior levels of an entity are aware of the risk management practices of the entity and personally accountable for compliance with this regime."[21] auDA believes that the same outcome is achieved where a Board resolves to approve the annual report and then the annual report is signed by a person duly authorised, such as the Board

[18] Security Legislation Amendment (Critical Infrastructure) Bill 2020, s30AG(2)(e)
[19] Ibid 48[306]
[20] Security Legislation Amendment (Critical Infrastructure) Bill 2020, s30AG(2)(f)
[21] Explanatory Document, Security Legislation Amendment (Critical Infrastructure) Bill 2020, 49[307]

Chair. The Bill needs to provide some flexibility as to how a Board or governing committee certifies the annual report.

Notification of cyber security incidents

34. auDA notes that the sector specific guidance on what constitutes a critical cyber security incident will be pivotal to understanding when the obligations under section 30BC are triggered.[22] At the moment, it is unclear as to when a cyber security incident meets the requisite harm threshold for classification as a critical cyber security incident. The Explanatory Document provides that "determining whether an incident is having a significant impact on the availability of the asset will be a matter of judgement for the entity."[23]

35. auDA is also concerned about the requirement to report a critical cyber security incident to ASD using the approved forms (written report and oral record) within the required time. As these forms are not yet available, it is difficult to assess the nature of the information that must be provided. auDA notes, that as a relatively small organisation, the priority of its technical staff will be to mitigate any harm to the .au DNS and assets as the incident is occurring and then assessing and repairing any systems or asset damage post incident. As such, auDA believes that the 12 hour reporting requirement is too onerous and should be replaced with 'as soon as practicable.' auDA notes that where a report is given orally that a written report must be provided to ASD within 48 hours.

Enhanced Security Obligations

Systems of National Significance

36. Systems of national significance (SoNS) "are of the highest criticality due to their national significance. These systems are so integral to the functioning of modern society that their compromise, disruption or destruction would have significant adverse impacts on Australia's economic and social stability, defence and national security."[24] It is the criticality of these systems to Australia that justifies the imposition of additional security obligations (Enhanced Security Obligations), including system information gathering notices.

---

[22] Ibid 50[319]

[23] Ibid

[24] Explanatory Document, Security Legislation Amendment (Critical Infrastructure) Bill 2020, 67[431]

37. Given the purported criticality of these systems, it is surprising that the only requirement for the Minister to declare a CI asset to be a SoNS, is that he or she is satisfied that the asset is of national significance. The Bill does not define the term 'national significance' so it must be given its ordinary or dictionary meaning. The Oxford English Dictionary describes 'national' as 'of a nation' and significance as 'of importance'. Therefore, a CI asset may be considered of national significance if it is 'important to the nation.' This threshold appears to be too low as, by definition, all CI assets are critical to the social and economic stability of Australia or its people, the defence of Australia, or national security.[25]

38. The Minister in determining whether a CI asset is of national significance must have regard to:

    a) If the Minister is aware of one or more interdependencies between the asset and one or more other CI assets - the nature and extent of those interdependence; and
    b) such matters (if any) as the Minister considers relevant.

However, these matters are not determinative of whether a CI asset is a SoNS.

39. auDA questions the utility of the distinction between CI assets, and SoNS, other than as mechanism to 'switch on' the Enhanced Security Obligations for any CI asset, irrespective of the criticality of that asset. auDA strongly advocates for the inclusion of a third limb under section 52B(1), requiring that the Minister must be satisfied that any 'compromise, disruption or destruction of the asset would have significant adverse impacts on Australia's economic and social stability, defence and national security"[26] As the Enhanced Security Obligations are focused on building the resilience and capability of SoNS to respond to cyber security incidents, the relevant impact should be assessed by reference to cyber security incidents.

<u>Access to systems information</u>

40. auDA is concerned that access to systems information may inadvertently capture data that may be considered personal information within the meaning of the *Privacy Act 1988* (Cth). What DNS data may be classified as personal data has

[25] Security of Critical Infrastructure Act 2018, s9(3)

[26] Explanatory Document, Security Legislation Amendment (Critical Infrastructure) Bill 2020, 51[325]

become more complex following the *Privacy Commission v Telstra Corporation Limited* (2017) FCAFC 4, where the court found that information (metadata) is only personal information when it is about an individual. The DNS data not only captures data relating to Australians but also foreign entities and individuals, whose information (including metadata) might be protected under laws with extra-territoriality, such as the General Data Protection Regulation.

Government Assistance

41. The Explanatory Document describes the information gathering, directions and intervention powers under Part 3A as a 'last resort power' or 'emergency mechanism'[27] for the Government to respond to the "most serious cyber security incidents which are affecting critical infrastructure assets and where the relevant entity is unwilling or unable to do so." [28] auDA welcomes the Government's commitment that the use of these powers should be subject to stringent safeguards and limitations to ensure they are "only used in the most serious circumstances."[29]

Authorisation framework

42. auDA has significant reservations about the authorisation framework for the exercise of powers under section Part 3A. auDA reiterates that the use of powers under Part 3A should only be authorised by a judicial officer as it provides a degree of independence and rigour. This approach would be consistent with the exercise of other coercive powers under the *Regulatory Powers (Standard Provisions) Act 2014*(Cth), and the *Crimes Act 1914* (Cth).

43. auDA considers that the proposed authorisation framework does not contain sufficient safeguards, given the exclusion of authorisation decisions from judicial review under the ADJR. auDA recommends that there should be some form of a judicial review and confirmation mechanism for an authorisation decision. auDA is attracted to judicial review and confirmation of a Ministerial authorisation, where the duration of that authorisation exceeds five days. This will ensure that these powers are only used to deal with 'emergency' situations and for no longer than necessary. The judicial officer would be required to review and confirm that the

[27] Explanatory Document, Security Legislation Amendment (Critical Infrastructure) Bill 2020, 55[361]
[28] Ibid 56 [363]
[29] Ibid

authorisation decision was open to the Minister on the grounds and facts provided by the Secretary in his/her application. Where a judicial officer finds that the decision was not open to the Minister on the grounds contained in the application, then the authorisation would be cancelled from the date of judicial review. This would not invalidate any acts taken prior to cancellation. auDA also considers that any successive fresh authorisation for the same entity in relation to the same cyber security incident should be subject to judicial review and confirmation before coming into force.

44. If the proposed authorisation framework is retained, auDA recommends reducing the duration of a Ministerial authorisation to a maximum of five days to reflect the emergency nature of these powers, which are designed to provide an immediate response to a serious cyber security incident. Section 25AG (4) provides that the Minister may give a fresh Ministerial authorisation in relation to the incident and asset. auDA believes that this is sufficient to deal with incidents that amount to a 'cyber campaign' or where the impact of the cyber security incident on the asset and other dependent critical infrastructure assets is still being manifested. It will also require the Minister to reassess the situation and provide for an additional round of consultation with the entity, which may identify problems with any previous authorisations and associated requests.

45. auDA acknowledges that there are additional measures in the Bill, which place a positive duty on the Minister to revoke the authorisation where the Minister is satisfied that it is no longer required;[30] and the Secretary to revoke a direction and an intervention request where he or she is satisfied that it is no longer required to respond to the cyber security incident to which the Ministerial authorisation relates.[31] However, these measures provide little comfort that directions and intervention requests will not continue beyond what is 'absolutely' necessary to deal with the immediacy of a cyber security incident.

Last resort powers

[30] Security Legislation Amendment (Critical Infrastructure) Bill 2020, s35AH

[31] ibid ss35AS(3), 35BA(3)

46. auDA welcomes the Government's commitment that action directions and intervention requests will only be authorised as a 'last resort' measure[32] where an entity is unable or unwilling to act.[33] The Explanatory Guide provides the following explanation "the owner or operator of the asset has primary responsibility for the asset, with the Government's responsibility *only being enlivened where their willingness or inability to respond* to an incident is having flow on impacts to Australia's national interests" (italics mine).[34] Given this statement, and the draft provisions, the key question is when and how the entities "unwillingness or that it is unable to act' is assessed. auDA assumes that this can be assessed at two key points of the authorisation process: (1) prior to the Secretary making an application, or (2) at the time the Minister must consult before making an authorisation under section 35AD.

47. As the authorisation process is triggered by an application by the Secretary,[35] auDA believes that it is at this stage that the Secretary should be required to consult with the affected entity where the application relates to an intervention request or action directions. There should be a statutory requirement for the application to set out the consultation that has been undertaken with the entity, and whether the entity has expressed any concerns, issues or expressed that it is unwilling or unable to voluntarily take the action. However, a disagreement as to best or most expedient technical or operational approach to mitigating the risk should not be considered an 'unwillingness or being unable to act.' The Secretary should only be permitted to apply where there is sufficient evidence of the entity's unwillingness or inability to act.

48. The Bill provides that the Minister may dispense with consultation with an entity where it would frustrate the effectiveness of a Ministerial authorisation for action directions or intervention request.[36] If the Minister exercises this power, then auDA is unclear as to how the Minister can form the mental state (satisfaction) that an entity is unwilling or unable to act that enlivens the authorisation power.

Self-incrimination and self-exposure

[32] Explanatory Document, Security Legislation Amendment (Critical Infrastructure) Bill 2020, 55[360]
[33] Security Legislation Amendment (Critical Infrastructure) Bill 2020, s35AB(7), 35AB(10)
[34] Explanatory Document, Security Legislation Amendment (Critical Infrastructure) Bill 2020, 60 (390)
[35] Security Legislation Amendment (Critical Infrastructure) Bill 2020, s35AF
[36] Ibid ss35AB(2), 35AD(2)

49. auDA is concerned that the Bill abrogates the privilege against self-exposure to penalties for individuals in respect to the requirement to provide information under section 35AK, system information periodic or system event-based reporting notices under section 30BD and a system information software notice. This means that information provided by an individual may be used against that individual or third parties in other civil and criminal proceedings. The Explanatory Document is silent on the policy justifications for abrogating this privilege, although the Department has advised that it is to capture rogue employees that may be involved in espionage or other activities and where the information may be useful for the purpose of criminal prosecution. However, auDA does not believe that this justifies the abrogation of the privilege.

50. auDA recommends that the Bill contain a use and derivative use immunity for individuals that covers both criminal and civil proceedings. auDA believes that there is sufficient scope to carve out specific criminal offences where the information should be allowed to be used in criminal proceedings relating to espionage and terrorism offences. The derivative use immunity should expressly apply to any information, document or thing obtained as a direct or indirect consequence of a requirement to provide information under the Bill.

.au Domain Administration Ltd
www.auda.org.au

PO Box 18315
Melbourne VIC 3001
info@auda.org.au