February 2020

Security Legislation Amendment (Critical Infrastructure) Bill 2020

Parliamentary Joint Committee on Intelligence and Security

.auDA

Executive Summary

The .au Domain Administration Limited (auDA) is the administrator of and the Australian self-regulatory policy body for the .au country code Top Level Domain (.au ccTLD). auDA operates under Terms of Endorsement issued by the Australian Government and is required to manage the .au domain in the public interest. auDA is a not-for-profit, private sector organisation that works with many stakeholders including the technical community, industry, civil society, government and the Australian and international community to develop and administer the rules for domains in the .au country code Top Level Domain (ccTLD). auDA manages the operation of the critical technical functions associated with the .au domain name system (DNS).

auDA supports the Government's policy objectives in relation to reforms to the *Security of Critical Infrastructure Act 2018* to prevent, mitigate and defend critical infrastructure from cyber-attack, and welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Intelligence and Security.

However, auDA considers that the Security Legislation Amendment (Critical Infrastructure) Bill 2020 in its current form has a number of provisions that are unclear or inappropriate. In particular, auDA has concerns about:

- The reliance on subordinate legislation to prescribe matters that are significant to the operation of the critical infrastructure scheme.
- The breadth of the information gathering powers.
- Cyber security incident notifications.
- Software installation by the Government. and the potential implications for privacy and surveillance, as well as the potential to inadvertently compromise network security.
- The threshold for a critical infrastructure asset to be declared a system of national significance.
- The abrogation of privilege against self-exposure to penalties for individuals.

auDA considers that the Bill does not strike an appropriate balance between critical infrastructure protection and the rights and obligations of all parties and the Australian Government's commitment to an open, free and secure Internet. Our submission includes recommendations to reduce this imbalance, including:

- a statutory requirement for the Minister to consult with affected entities before the making of rules that apply to them, to ensure that the rules are proportionate, effective and technically feasible. auDA considers it important that the rules do not adopt a one-size-fits-all approach, and is committed to working with the Government to co-design sector specific rules for the communications sector, and more specifically, entities that manage Australian Top Level Domain (TLD) systems.
- tightening the provisions relating to the use and disclosure of protected information similar to the secrecy and access provisions under Part 11 of the *Anti-money Laundering and Counter Terrorism Financing Act 2006* (Cth).
- With respect to notifying cyber security incidents that have a *significant impact* on the availability of an asset, providing a definition of *significant impact* that includes the impact of the incident on the availability of the asset, and the potential cascading impact of the asset being unavailable.
- With respect to notifying cyber security incidents that have a *relevant impact* on the asset, the definition of *relevant impact* should have a more robust threshold that requires the relevant impact to have a material effect on or compromises the asset or data.
- allowing an entity to disclose protected information for the purpose of complying with another Australian law.
- the Government's ability to compel an entity to install software on its systems should only be exercised where the information may assist in determining the exercise of powers under Part 2C and 3A of the Act.
- requiring a threshold assessment that the degradation, destruction or disruption of an asset would result in serious damage to Australia's national interests before a critical infrastructure asset is declared a system of national significance.
- greater transparency and accountability mechanisms around Ministerial declarations of systems of national significance, and a right of merits review in the Security Division of the *Administrative Appeals Tribunal.*
- the Government should have a positive duty to take all reasonable steps to protect unauthorised access, use or disclosure of information collected pursuant to the Act. auDA recommends a provision similar to section 127(1) of the Australian Securities and investment Commission Act 2001 (Cth),
- inclusion of a use and derivative use immunity for individuals that covers both criminal and civil proceedings.

Preventing and defending Australia's critical infrastructure from cyber-attack is vitally important and auDA appreciates the opportunity to engage with government on this matter. To this end, we would be pleased to meet with the Committee and speak to our

submission or provide additional information on any related matters the Committee seeks to explore.

Submission

1. .au Domain Administration Limited ('auDA') welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Intelligence and Security's (PJCIS) review of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 ('the Bill'). auDA also made submissions to the Department of Home Affairs Consultation Paper *Protecting Critical Infrastructure and Systems of National Significance*, and the Exposure Draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020. These submissions are attached and provide detailed information on the role and functions of auDA as the administrator of the .au country code Top Level Domain (.au ccTLD), the Domain Name System ('the DNS') and the global and distributed nature of the .au DNS.

2. auDA is supportive of the Australian Government's policy objectives behind the reforms to the *Security of Critical Infrastructure Act 2018,* which is to prevent, mitigate and defend critical infrastructure from cyber-attack. These policy objectives align with the Australian Government's commitment to implementing the Norms of Responsible State Behaviour in Cyberspace[1] ('the Norms') to promote "an open, secure, stable, accessible and peaceful ICT environment" [2] through, among others, the protection of critical infrastructure[3] and responsible reporting of ICT vulnerabilities.[4] However, as the .au ccTLD administrator, auDA does not believe that the Bill strikes an appropriate balance between critical infrastructure protection, the rights and obligations of all parties and the Australian Government's commitment to "an open, free and secure internet." [5]

---

[1] *Developments in the field of information and telecommunications in the context of international security.* UN GAOR A/RES/70/237, 23 December 2015.

[2] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN GAOR A/70/174 [2]

[3] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN GAOR A/70/174[13(g)]

[4] Ibid[13(j)]

[5] Australian Government, Department of Foreign Affairs, Australia's International Cyber Engagement Strategy (2016) https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/part_5_internet_governance_and_cooperation.html; Australian Government, Department of Home Affairs, Five Country Ministerial communique 2018 <https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/five-country-ministerial-2018#:~:text=of%20online%20spaces-,We%2C%20the%20Homeland%20Security%2C%20Public%20Safety%2C%20and%20Immigration%20Ministers,extremists%20and%20other%20illicit%20actors>

3. All references to sections of the *Security of Critical Infrastructure Act 2018* ('the Act') should be read as sections as amended or inserted by the Bill.

.au Domain Administration Limited (auDA)

4. auDA is the administrator of and the Australian self-regulatory policy body for the .au country code Top Level Domain (ccTLD). auDA performs this role pursuant to the Australian Government Terms of Endorsement[6] and the Internet Corporation for Assigned Names and Numbers (ICANN) Sponsorship Agreement.[7] In performing these functions, auDA has:

    (a) international obligations to manage the universality, interoperability and accessibility of the Public Core of the Internet; and

    (b) domestic obligations to manage the .au ccTLD in the public interest for the benefit of all Australians, subject to Australian Government requirements.

5. The division of responsibilities between the Australian Government and ICANN is:

    (a) the Australian Government has responsibility for overseeing the interest of Australia and its Internet community in the .au ccTLD [8]; and

    (b) ICANN has responsibility for preserving the technical stability and operation of the DNS and Internet in the interest of the global Internet community[9].

6. The .au ccTLD is hierarchically organised into second level domains (including com.au, net.au, org.au, asn.au, id.au, edu.au, gov.au, vic.au and csiro.au). The edu.au and gov.au domains also comprise child zones which are allocated to or used by State and Territory Governments, such as justice.vic.gov.au. auDA has delegated the management of the gov.au to the Commonwealth of Australia through the Digital Transformation Agency (DTA). DTA has arrangements with the

---

[6] Australian Government, Department of Communications and the Arts, Review of the .au Domain Administration: Terms of Endorsement (issued 16 April 2018) <https://www.communications.gov.au/documents/review-au-domain-administration-terms-endorsement>

[7] Internet Corporation for Assigned Names and Numbers, ccTLD Sponsorship Agreement (.au) (25 October 2001) < https://www.icann.org/resources/unthemed-pages/sponsorship-agmt-2001-10-25-en>

[8] Australian Government Terms of Endorsement (dated 31/12/2000); Clause 1.10 of the ccTLD Sponsorship Agreement (.au) (https://www.icann.org/resources/unthemed-pages/sponsorship-agmt-2001-10-25-en); Paragraph 4.1.1 of the Government Advisory Committee, Internet Corporation for Assigned Names and Numbers, Principles and Guidelines for the Delegation and Administration of Country Code Top Level Domains (5 April 2005); https://gac.icann.org/principles-and-guidelines/public/principles-cctlds.pdf

[9] Internet Assigned Numbers Authority, IANA Report on request for Redelegation of the .au Top Level Domain (31 August 2001) https://www.iana.org/reports/2001/au-report-31aug01.html; Clause 1.10 of the ccTLD Sponsorship Agreement (.au) (https://www.icann.org/resources/unthemed-pages/sponsorship-agmt-2001-10-25-en

State and Territory Governments relating to the administration of their third level domain (vic.gov.au, nsw.gov.au, act.gov.au, qld.gov.au, nt.gov.au, wa.gov.au, sa.gov.au and tas.gov.au).

Public Core of the Internet

7. The Domain Name System (DNS) is part of the *Public Core of the Internet*, which comprises the following layers:

   (a) Logical layer – applications, data and protocols that allow exchange of data, such TCP/IP, DNS and routing protocols

   (b) Physical layer compromising the physical network components (hardware and other infrastructure, such as telecommunications cables, internet routers, DNS nameservers and computers)

   (c) Organizational layer such as internet exchanges, Computer Emergency Response Teams (CERTs) (e.g. CERT Australia), domain name registrars, Top Level Domain (TLD) Registries (e.g. .au registry), TLD administrators (e.g. auDA), and policy settings.

8. The Public Core of the Internet only works properly if its underlying values of universality, interoperability and accessibility are guaranteed through the promotion of data security, ie confidentiality, integrity and availability.[10] These principles and values are reflected in the Australian Government's definition of an "open, free and secure" cyberspace as:

   > "An **open** cyberspace is interoperable across borders and accessible to all; it facilitates unrestricted participation and the free flow of information, driving inclusive online collaboration, innovation and growth.
   >
   > A **free** cyberspace means people are not burdened by undue restrictions on their access to and use of cyberspace; and their human rights are protected online as they are offline so that

[10] Government of France, Ministere De L'Europe Et Des Affaires Etrangeres, Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cybersapce <https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in>; Australian Government, Australia's international Cyber Engagement Strategy (2016) 2019 Progress Report [5.01] https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/2019_progress_report.html

cyberspace remains a vibrant force for economic, social and cultural development.

A **secure** cyberspace is safe, reliable and resilient; it fosters an environment of trust so that individuals, businesses and governments can engage online with confidence and realise the opportunities and minimise the risks of the digital age."[11]

9. These principles also underpin the *UN Norms of Responsible State Behaviour in Cyberspace*, which require States to strike an appropriate balance between critical infrastructure protection and human rights, including the right to privacy. States are urged to respect "Human Rights Council resolutions 20/8 and 16/13 on the promotion, protection and enjoyment of Human Rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights."[12]

10. The Australian Government has always recognised that a multi-stakeholder model is the most effective way of dealing with the complex policy and technical challenges associated with the Internet, in particular security concerns.[13] auDA supports this position as the DNS is a globally distributed network that crosses jurisdictional boundaries, and an impact (whether regulatory or a security incident) on one part of this global network may have flow on consequences for infrastructure and citizens in another jurisdiction.

CONCERNS

Reliance on subordinate legislation

11. The Senate Standing Committee on the Scrutiny of Bills expressed reservations about the Bill's reliance on subordinate legislation to prescribe matters which are significant to the operation of the critical infrastructure scheme.[14] auDA agrees with this view, noting that consultation with regulated entities and critical

[11] Australian Government, Department of Foreign Affairs, Australia's International Cyber Engagement Strategy (2016) https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/part_5_internet_governance_and_cooperation.html
[12] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN GAOR A/70/174[13(e)]
[13] Australian Government, Department of Foreign Affairs, Australia's International Cyber Engagement Strategy (2016) https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/part_5_internet_governance_and_cooperation.html
[14] Senate Standing Committee for the Scrutiny of Bills, Parliament of Australia, Scrutiny Digest 2 of the 2021, 3 February 2021, 22-24

infrastructure sectors will be essential to ensure rules which are proportionate, effective, and technically feasible. To achieve this, **auDA believes there should be a statutory requirement to consult with affected entities before the Minister makes the rules.**

12. There is no requirement under section 61 of the Act for the Minister to consult with affected parties or to take certain matters into consideration prior to making rules. However, sections 18AA, 30ABA and 30AL of the Act impose minimal consultation requirements for rules relating to prescribing an asset as a critical infrastructure asset, and critical infrastructure risk management programs, respectively. The Minister must publish the draft rules on the Department's website and invite submissions from interested persons within 28 days. There is no requirement for the Minister to be satisfied of any specific matters prior to making the rules.

13. Sub-section 30AL(3) of the Act provides the Minister may waive the requirement to consult on rules relating to critical infrastructure risk management programs, if satisfied that:

    (a) there is an imminent threat that a hazard will have a significant relevant impact on a critical infrastructure asset; [15] or

    (b) a hazard has had, or is having, a significant relevant impact on a critical infrastructure asset. [16]

14. The Explanatory Memorandum provides that the "potential urgency of the situation and the significance of the impact, and the flow on impacts to Australia's economy, society, and defence, warrant this departure from standard process." auDA believes this argument is problematic for the following reasons:

    (a) updating a written critical infrastructure risk management program does not appear to be an effective mechanism for dealing with an imminent or live threat.

    (b) regulated entities are best placed to determine what mitigation strategies will or are appropriate to deal with threats to their infrastructure, and waiving the consultation obligations may result in inappropriate, or disproportionate measures.

    (c) there appears to be no urgency to justify the waiver of consultation requirements where a threat has already occurred.

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

15. **auDA believes the Ministerial authorisation powers relating to action directions under section 35AQ of the Act would be a more appropriate and effective mechanism to deal with these emergency situations**.

16. Regulated entities must rely on the consultation requirements under section 17 of the *Legislation Act 2003*(Cth) for all other matters to be prescribed by the rules. 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[17] and persons likely to be affected by the rule.[18] **auDA does not believe that this statutory consultation requirement is adequate for the development of rules that may be technically complex, and may have a significant impact on the operations of a regulated entity.**

17. **auDA recommends that section 61 of the Act be amended to include specific consultation requirements before the Minister may make rules**, including:

    (a) a minimum consultation period of 28 days before any rule can be made.

    (b) requires the Department to notify all responsible entities entered on the Register of Critical Infrastructure Assets and any party that is likely to be affected by the rules.

    (c) the Minister must take into consideration the technical feasibility, and resource and financial costs of complying with proposed rules.

18. It is important any rules take into consideration the different sub-sectors within a critical infrastructure sector and that rules do not adopt a one-size fits all approach. **auDA is committed to working with the Government to co-design sector specific rules for the communications sector and more specifically entities that manage Australian Top Level Domains (TLD).**

Information gathering powers

19. auDA has concerns regarding the breadth of the information gathering powers exercised by the Secretary, and the non-exhaustive list of persons to whom the Secretary may disclose this information for purposes other than critical

[17] *Legislation Act 2003* (Cth), s17(2)(a)
[18] Ibid s17(2)(b)

infrastructure protection.[19] These concerns relate not only to the ambit of specific powers, but to issues relating to the Department's security and management of this information, including unauthorised access, disclosure of information or any other misuse of records. A potential data breach could have serious ramifications for the commercial interests and security of a regulated entity as well as broader Australian interests, such as national security and privacy.

20. Given the highly sensitive commercial and technical information about an entity collected pursuant to these powers, auDA believes the current use and disclosure of protected information provisions are insufficient to protect the legitimate interests of regulated entities. auDA is particularly concerned protected information can be disclosed to Ministers, their staff and agencies where the Minister has responsibility for, among others, industry policy and promoting investment in Australia. While this may have been considered acceptable under the existing critical infrastructure protection regime, **auDA believes the expansion of information gathering powers and the sensitivity of the information gathered warrant a higher threshold for use and disclosure**, especially given the justification for these powers is to protect Australia's national interest.

21. **auDA recommends the PJCIS considers tightening the use and disclosure of protected information provisions along the lines of the secrecy and access provisions under Part 11 of the *Anti-Money Laundering and Counter Terrorism Financing Act 2006* (Cth) (the 'AML/CTF Act').** In particular, the secondary disclosure provisions under sections 128 and 131 of the AML/CTF Act and the provisions governing when information can be disclosed to a foreign country under section 132 of the AML/CTF Act.

Cyber security incident notifications

22. auDA supports in principle an obligation to notify ASD of a critical cyber security incident that has a significant impact on the availability of an asset under section 30BC of the Act. However, auDA believes the provision as currently drafted lacks clarity and certainty as to when the notification obligation arises and expresses concern at the requirement to notify the relevant government body within 12 hours of an entity becoming aware of the incident.

23. The notification obligation only arises where a cyber security incident is having a significant impact on the availability of an asset. The Bill does not define a

[19] Security of critical Infrastructure Act 2018, s42. The Secretary may disclose protected information to Ministers, and their staff, and government agencies responsible for taxation, law enforcement, corporate regulation, industry policy and promoting investment in Australia.

significant impact, which if given its ordinary English meaning is "an important or consequential effect." [20] However, the Explanatory Memorandum ('the EM') implies that a significant impact on the availability of an asset must also be assessed by reference to the potential impact on the provision of essential services and cascading "impacts across the economy or the sector."[21] The EM provides the following illustration "For example, a cyber security incident which affects the availability of critical clearing and settlement facility for a very brief period may have significant repercussions, while an incident that affects the availability of a critical education asset for the same period of time may have a substantially lower impact." [22]

24. auDA does not believe it is appropriate to leave the obligation to notify government of a critical cyber security incident to the "judgement of the responsible entity,"[23] given the failure to notify attracts a civil penalty and enlivens the regulatory powers of the Department. **auDA recommends the PJCIS considers amending the threshold requirement of significant impact to include**:

    (a) the impact of the incident on the availability of the asset; and

    (b) the potential cascading impact of the asset being unavailable on essential services, the economy, defence and national security of Australia.

25. auDA notes the obligation to notify government of an incident within 12 hours only arises when the entity becomes aware of the significant impact on the availability of the asset. This recognises that "determining the significance of the impact may take some time." [24] This implies considerable time may lapse between the incident and the notification to government, and appears to be counterintuitive to the criticality of these incidents. auDA also notes that if the investigation of the incident may take more than 72 hours to assess its significance, that the entity would have already notified government of the incident under section 30BD of the Act. **auDA recommends the PJCIS considers a uniform 72 hour reporting window for critical and other cyber security incidents**.

[20] *Australian Oxford Dictionary* (2nd ed 2004), 1204, 627
[21] Explanatory Memorandum, Security Legislation Amendment (Critical Infrastructure) Bill 2020 [645]
[22] Ibid [642]
[23] Ibid
[24] Ibid [644]

Cyber security incident

26. An entity also has an obligation to notify government of cyber security incidents that are imminent, occurring or have occurred that have a relevant impact on the asset. Section 8G of the Act defines a relevant impact as any impact (direct or indirect) of the cyber security incident on the availability, integrity or the reliability of the asset, or the confidentiality of information or data about or stored in the asset or computer data. auDA believes the definition of relevant impact is overly broad and may be interpreted to include simple things like improper password sharing by employees. **auDA advocates for a more robust threshold that requires the relevant impact to have a material effect on or compromises the asset or data.**

27. auDA observes that a cyber security incident under section 30BD of the Act may also trigger notification requirements under the Notifiable Data Breach Scheme set out in Part IIIC of the *Privacy Act 1988* (Cth), continuous disclosure requirements relating to market sensitive information under the *Corporations Act 2001* (Cth) and ASX Listing Rules and the reporting obligations under the APRA Prudential Standard CPS 234. A report under sections 30BC and 30BD is protected information under section 41 of the Act, which an entity may only use and disclose for the purpose of performing its functions or duties under the Act, or otherwise ensuring compliance with a provision of the Act. **auDA recommends that section 41 of the Act be amended to allow the entity to disclose protected information for the purpose of complying with another Australian law**.

Periodic and event-based reporting and software installation

28. The .au ccTLD is part of the public core of the internet and operates on the principle of universality, interoperability and accessibility and the promotion of data security, including integrity and privacy. In 2013, the Snowden revelations of the US Government's surveillance of the DNS resulted in key internet infrastructure organisations releasing the Montevideo Statement on the Future of Internet Cooperation, which expressed "strong concern over the undermining of the trust and confidence of Internet users globally due to recent revelations of pervasive monitoring and surveillance."[25] The Snowden revelations also triggered the

[25] Internet Corporation for Assigned Names and Numbers, Montevideo Statement on the Future of Internet Cooperation https://www.icann.org/news/announcement-2013-10-07-en (accessed 23 February 2013).

completion of the transition of the Internet Assigned Numbers Authority to ICANN from the US Government.[26]

29. The Internet Engineering Taskforce ('IETF'), the standards setting body for internet infrastructure, released RFC 6973 *Privacy Considerations for Internet Protocols* and RFC 7624 *Confidentiality in the Face of Pervasive Surveillance,*[27] which provide a detailed explanation of the vulnerabilities in Internet protocols, software and hardware exploited by the NSA for monitoring and surveillance purposes. A simple example is the monitoring of DNS queries of users which can reveal which services they are using and which websites they are visiting as well as other transaction data such as the user's IP address, location and time of request. This metadata can disclose sensitive information seeking practices related to, among others, medical or health conditions, and political affiliations or ideology.[28] auDA is cognisant that these DNS vulnerabilities have not been resolved and that any monitoring of DNS or Internet traffic can potentially provide a wealth of information about a user's habits and when combined with other data sources can identify individual users.[29] auDA is concerned to ensure that access to systems information necessary to protect critical infrastructure through the identification of malicious activity, and surveillance does not lead to monitoring of users through DNS queries.

30. Sections 30DB, 30DC and 30DJ provides that the Secretary can by written notice require a regulated entity to provide a report or install software on their systems to provide information that relates to the operation of a computer, and which may assist with determining whether a power should be exercised in relation to a system of national significance (SoNs) and is not personal information (within the meaning of the *Privacy Act 1988* (Cth)). auDA has several concerns with the ambit of these provisions, and the technical feasibility of preparing systems

[26] US Government, National Telecommunications and Information Administration, Fact Sheet: The IANA Stewardship Transition Explained https://www.ntia.doc.gov/other-publication/2016/fact-sheet-iana-stewardship-transition-explained (accessed 23 February 2021)

[27] Internet Engineering TaskForce, RFC 7624 Confidentiality in the Face of Pervasive Surveillance: A threat Model and Problem Statement (2015) https://tools.ietf.org/html/rfc7624 (accessed 23 February 2021); Internet Engineering TaskForce, RFC 6973 *Privacy Considerations for Internet Protocols* (2013) https://tools.ietf.org/pdf/rfc6973.pdf (accessed 23 February 2021).

[28] Bradshaw, Samantha and Laura DeNardis, Privacy by Infrastructure: The Unresolved case of the Domain Name System, *Policy and Internet* 11(1) 18-31

[29] Bradshaw, Samantha and Laura DeNardis, Privacy by Infrastructure: The Unresolved case of the Domain Name System, *Policy and Internet* 11(1) 18-31

information reports or installing software that does not inadvertently capture personal information.

31. **auDA considers the use of these access to system information provisions to "assist with determining whether a power under this Act should be exercised in relation to a SoNS" is too broad given the numerous powers that may be exercised under the Act, and should be narrowed to specified powers, such as those under Part 3A of the Act. auDA believes the Government's ability to compel an entity to install software on its systems under section 30DJ of the Act should only be exercised where the information may assist in determining the exercise of powers under Part 2C and 3A of the Act**. There are significant risks to an entity from the installation of third party software on its systems, which may inadvertently threaten or compromise the security of the network.

32. auDA believes it may be difficult in practice to provide reports on systems information that does not include personal data, especially in respect to DNS metadata. Currently, there is considerable legal uncertainty as to whether technical data or metadata collected in relation to individuals is personal information within the meaning of the *Privacy Act 1988* (Cth). While the Full Federal Court's judgement in *Privacy Commission v Telstra Corporation Limited* (2017) FCAFC 4, found that telecommunications metadata was not personal information (on the basis that it failed to satisfy the threshold of whether the information was about an individual.[30]), it is understood that whether metadata is about an individual will depend on the facts of any individual case.[31]

33. The Attorney General's Department is undertaking a review of the *Privacy Act 1988* (Cth), which includes whether the definition of personal information should be extended to include metadata and online identifiers.[32] The Australian Competition and Consumer Commission in its Digital Platforms Inquiry recommended that the "definition of personal information in the [Privacy] Act be updated to clarify that it captures technical data such as IP addresses, device identifiers, location data and any other online identifiers that may be used to identify an individual."[33]

34. auDA also notes approximately 74 percent of daily DNS queries to its servers originate from overseas jurisdictions, such the European Union. The systems information held by auDA therefore captures data relating to foreign entities and individuals and this technical information may be protected under laws with extra-territoriality. For example, article 4 of the European Union General Data

[30] *Privacy Commissioner v Telstra Corporation Ltd* (2017) FCAFC 4 [63]
[31] Ibid [63]
[32] Attorney General's Department, *Issues Paper:* Review of the *Privacy Act 1988* (Cth) (30 October 2020), 18-21
[33] Australian Competition and Consumer Commission, *Digital Platforms Inquiry – Final Report* (Part 1), 24

Protection Regulation (GDPR) defines personal data as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Systems of National Significance

35. The Explanatory Memorandum describes systems of national significance as a "subset of critical infrastructure assets that have an additional element of criticality based on their national significance."[34] It is the criticality of these assets to Australia that justifies the imposition of additional security obligations under Part 2C (Enhanced Security Obligations), including system information gathering notices. The criticality of an asset is assessed by reference to the potential consequences that would arise for the social and economic stability of Australia and its people, Australia's defence and national security from a hazard having a significant impact on the availability, integrity, reliability and confidentiality of data of the asset.[35]

36. **auDA believes the "criticality threshold' under sub-section 52B(2)(a) of the Act is too low**, given a critical infrastructure asset is defined as an asset that "is critical to the social or economic stability of Australia or its people; or the defence of Australia or national security."[36] It is arguable that hypothetically any significant impact on the availability, reliability, integrity and confidentiality of data would have consequences for Australia's social and economic wellbeing, defence or national security. **auDA considers the 'criticality threshold' should require an assessment of whether the degradation, destruction, or disruption of the asset would result in serious damage to Australia's national interests**.[37]

37. auDA acknowledges section 52E of the Act provides an entity with a right to seek an internal review of a Ministerial declaration that an asset is a SoNS. There are several issues with the proposed internal review mechanism, including:

    (a) internal reviews conducted by the Secretary are advisory recommendations to the Minister, and do not have any legal status. The Minister has the sole discretion to accept or reject the recommendations.

[34] Explanatory Memorandum, Security Legislation Amendment (Critical Infrastructure) Bill 2020, [1179]
[35] Security Legislation Amendment (Critical Infrastructure) Bill 2020, ss 8G, 52B
[36] Security Legislation Amendment (Critical Infrastructure) Bill 2020, ss 9(3), 51
[37] Explanatory Memorandum, Security Legislation Amendment (Critical Infrastructure) Bill 2020, [1181]

(b) there are no requirements for transparency in the conduct by the Secretary of internal reviews. There is no requirement for the Secretary to provide the entity with a copy of its internal review and recommendations, nor is there an obligation for the Minister to provide written decisions to the entity where an application to have the declaration revoked is rejected.

38. auDA considers there should be greater transparency and accountability mechanisms around Ministerial declarations to limit regulatory creep. **auDA recommends a right of merits review in the Security Division of the *Administrative Appeals Tribunal* (AAT)**. This approach would be consistent with the existing right to seek merits review of an adverse security assessment by the Australian Security and Intelligence Organisation for the purposes of enlivening section 32 of the Act. auDA observes that while an entity may technically be able to seek a review of a Ministerial declaration under the *Administrative Decisions (Judicial Review) Act 1977* (Cth), that section 41 of the Act would appear to prohibit the disclosure of a Ministerial declaration for the purposes of legal proceedings.

Protected Information

39. As set out above, **auDA strongly advocates for the revision of the protected information use and disclosure provisions along the lines of the secrecy and access provisions under Part 11 of the AML/CTF Act**. If this recommendation is not accepted, then **at a minimum, the existing provisions should be amended** to include:

    (a) the right of an entity to voluntarily disclose protected information for the purpose of obtaining legal advice and commencing or responding to any legal proceedings in relation to the Act, such as being sued for damages by a third party as a result of an entity complying with an action direction under section 35AQ of the Act.

    (b) disclosure for the purpose of complying with an Australian law.

    (c) the ability for the Secretary to impose conditions on the secondary use and disclosure of protected information that has been disclosed pursuant to sections 42, 43, and 43A of the Act.

40. **auDA believes that the Government should have a positive duty to take all reasonable steps to protect unauthorised access, use or disclosure of information collected pursuant to the Act. auDA recommends a provision similar to section 127(1) of the *Australian Securities and investment Commission Act 2001* (Cth),** which places a positive duty on the Australian Securities and Investment Commission to take all reasonable steps to prevent unauthorised disclosure of information.

Self-incrimination and self-exposure

41. auDA is concerned 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 information provided by an individual may be used against that individual or third parties in other civil and criminal proceedings.

42. **auDA recommends the Bill contain a use and derivative use immunity for individuals that covers both criminal and civil proceedings**. auDA believes 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

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, caroline.fritsch@auda.org.au.

Yours sincerely,

Rosemary Sinclair AM
CEO
.au Domain Administration Ltd

.au Domain Administration

Supplementary Submission to Department of Home Affairs *Protecting Critical Infrastructure and Systems of National Significance*

21 September 2020

.au DOMAIN ADMINISTRATION LTD

www.auda.org.au

PO Box 18315
Melbourne VIC 3001

info@auda.org.au

Contents

Executive Summary

- .au Domain Administration Limited (auDA) takes security extremely seriously and benchmarks against international best practice
- auDA's DNS systems are globally distributed for scale and reliability, and to handle the high proportion of international DNS queries for .au domains
- auDA accredited registrars are globally distributed
- The internet resources (including web and email servers) referenced by domain names in the .au ccTLD are globally distributed
- auDA has international obligations to manage and preserve the universality, interoperability and accessibility of the Public Core of the Internet
- The Australian Government's international position is that no government should regulate the Internet, and that a multi-stakeholder model of internet governance is the most effective mechanism to develop public policy positions across the full spectrum of cyber affairs
- auDA believes that the existing Australian Government terms of Endorsement and the reserve powers in the Telecommunications Act already provide sufficient mechanisms for the Government to provide oversight of auDA

Introduction

1. .au Domain Administration Limited (auDA) welcomes the opportunity to make a supplementary submission to the Department of Home Affairs *Protecting Critical Infrastructure and Systems of National Significance Consultation Paper.* This submission should be read in conjunction with the short submission made by auDA on 16 September 2020.

2. While auDA welcomes the Australian Government's policy commitment to an all-hazards approach to protecting critical infrastructure, the proposed critical infrastructure (CI) reforms are designed to enhance the capability of the government and critical infrastructure operators and owners to 'manage the national security risks of espionage, sabotage and coercion arising from foreign involvement in Australia's critical infrastructure.'[1] In this context, auDA believes that the application of these CI reforms to the .au ccTLD raises significant public policy issues relating to the securitization of the Internet.

3. auDA is willing to work with the Department of Home Affairs ('the Department') to identify the potential consequences of DNS infrastructure disruption and to establish appropriate risk mitigation strategies. auDA is happy to facilitate a workshop with the Department and auDA's accredited Registrars[2] and DNS infrastructure providers to work through the potential impacts of the CI reforms on the .au Domain Name System (DNS).

4. auDA has provided an overview of the Domain Name System and .au country code Top Level Domain (ccTLD) at Attachment A.

Background

.au Domain Administration Limited

5. auDA is the administrator of and the Australian self-regulatory policy body for the .au country code Top Level Domain (ccTLD). auDA performs this role pursuant to the Australian Government Terms of Endorsement[3] and the Internet Corporation for Assigned Names and Numbers (ICANN) Sponsorship Agreement.[4] In performing these functions, auDA has:

    (a) international obligations to manage and preserve the universality, interoperability and accessibility of the Public Core of the Internet; and

    (b) domestic obligations to manage the .au ccTLD in the public interest, subject to Australian Government requirements.

6. The division of authority between the Australian Government and ICANN is:

[1] Explanatory Memorandum, Security of Critical Infrastructure Bill 2017, 1 [1].
[2] auDA accredits Registrars to provide Registrar Services, including the registration of domain names.
[3] Australian Government, Department of Communications and the Arts, Review of the .au Domain Administration: Terms of Endorsement (issued 16 April 2018) <https://www.communications.gov.au/documents/review-au-domain-administration-terms-endorsement>
[4] Internet Corporation for Assigned Names and Numbers, ccTLD Sponsorship Agreement (.au) (25 October 2001) < https://www.icann.org/resources/unthemed-pages/sponsorship-agmt-2001-10-25-en>

(a) the Australian Government has sovereign rights over the delegation and administration of the .au ccTLD[5] ; and

(b) ICANN has authority over the global technical coordination to ensure that the Internet domain name system continues to provide an effective and interoperable global naming system[6].

Terms of Endorsement

7. The Australian Government Terms of Endorsement (TOE) provide that 'responsibility for the administration of .au is ultimately derived from and is subject to, the authority of the Commonwealth. The Australian Government can delegate the responsibility for managing the .au namespace to an appropriate entity or organization.'[7] The Australian Government endorsement of auDA as the .au administrator is contingent on auDA administering the .au in the public interest and performing the following core functions, among others:

- ensure stable, secure and reliable operation of the .au domain space
- respond quickly to matters that compromise DNS security[8]

8. In performing these functions, auDA is required to:

- engage with key international security fora to ensure it is aware of international security developments and best practice
- develop, maintain and, to the greatest extent possible, publish an enterprise security strategy which is informed by domestic and international best practice
- work with the Department of Communications and the Arts to facilitate partnerships between auDA and relevant cyber security agencies[9]

9. The Australian Government through the Department of Infrastructure, Transport, Regional Development and Communications (DITRDC) retains supervisory oversight of auDA, including:

- receiving quarterly reports on performance and work priorities
- right to independently review auDA's reporting and reporting processes at any time

[5] Australian Government Terms of Endorsement (dated 31/12/2000); Clause 1.10 of the ccTLD Sponsorship Agreement (.au) (https://www.icann.org/resources/unthemed-pages/sponsorship-agmt-2001-10-25-en); Paragraph 4.1.1 of the Government Advisory Committee, Internet Corporation for Assigned Names and Numbers, Principles and Guidelines for the Delegation and Administration of Country Code Top Level Domains (5 April 2005); https://gac.icann.org/principles-and-guidelines/public/principles-cctlds.pdf

[6] Internet Assigned Numbers Authority, IANA Report on request for Redelegation of the .au Top Level Domain (31 August 2001) https://www.iana.org/reports/2001/au-report-31aug01.html; Clause 1.10 of the ccTLD Sponsorship Agreement (.au) (https://www.icann.org/resources/unthemed-pages/sponsorship-agmt-2001-10-25-en

[7] Australian Government, Department of Communications and the Arts, Review of the .au Domain Administration: Terms of Endorsement (issued 16 April 2018) 1.

[8] Ibid

[9] Ibid 3

- a senior officer from the DITRDC is included in all relevant auDA governance processes, including, but not limited to, non-voting observer status at board meetings for all decisions.[10]

10. The Australian Government also has reserve powers under sections 474-477 of the *Telecommunications Act 1997* (Cth) and sections 11 and 17 of the *Australian Communications and Media Authority Act 2005* (Cth) to provide for intervention in the event that auDA is unable to manage electronic addressing in an effective manner.

ICANN Sponsorship Agreement

11. The ICANN Sponsorship Agreement sets out the technical responsibilities and obligations of ICANN and auDA in managing the .au ccTLD zone to ensure the "technical stability and operation of the DNS and Internet in the interest of the global internet community."[11] The ICANN Sponsorship Agreement requires auDA to:

    (a) to ensure the stable and secure operation and maintenance of the authoritative primary and secondary nameservers[12]

    (b) provide ICANN with access to zone files and registration data for the .au ccTLD for the purpose of verifying and ensuring the operational stability of the .au ccTLD[13]

    (c) ensure the safety and integrity of the registry database, including the establishment of an escrow or mirror site for the registry data[14]

    (d) requirement to keep the .au ccTLD technical and administrative contact details up to date

    (e) conformity to ICANN policies relating to the interoperability of the .au ccTLD with other parts of the DNS and Internet, operational capabilities and performance of auDA, and the obtaining and maintenance of, and public access to, accurate and up to date contact information for registrants[15]

    (f) comply with the technical specifications set out in Attachment F, including operating the database with accuracy, robustness and resilience.[16]

12. ICANN can terminate the Sponsorship Agreement where, among other matters:

    (a) auDA acts or continues acting in a manner that ICANN reasonably determined endangers the operational stability of the DNS or the Internet[17]

---

[10] Ibid
[11] Internet Corporation for Assigned Names and Numbers, ccTLD Sponsorship Agreement (.au) (25 October 2001) [1.10]
[12] Ibid[4.1]
[13] Ibid[4.2]
[14] Ibid[4.3]
[15] Ibid[4.5]
[16] Internet Corporation for Assigned Names and Numbers, ccTLD Sponsorship Agreement (.au) (25 October 2001), Attachment F <https://www.icann.org/resources/unthemed-pages/sponsorship-agmt-attf-2001-10-25-en>
[17] Internet Corporation for Assigned Names and Numbers, ccTLD Sponsorship Agreement (.au) (25 October 2001)[6.2.3]

(b) the Australian Government notifies ICANN that it has withdrawn its endorsement of auDA as an appropriate person to manage the .au ccTLD.[18]

13. On termination of the agreement, auDA has a surviving obligation to cooperate with ICANN to transfer the operation of the .au ccTLD to another party endorsed by the Australian Government.[19]

Corporate Constitution

14. auDA is required to operate within its Constitution under the Australian Government TOE. [20] The objects of the Constitution set out the technical and regulatory functions of auDA as the .au ccTLD administrator.

15. auDA technical functions are:

(a) 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,[21] and

(b) to manage the operation of critical technical functions including the primary and secondary nameservers, zone files for the second level domains (2LDs) and a searchable database (https://whois.auda.org.au/) containing information on registrations within the .au ccTLD.[22]

16. The self-regulatory policy functions, which enable auDA to make and enforce rules governing the accreditation of registrars and registry operators,[23] and the rules governing the registration of domain names in the second level domains (2LD)[24] are an important tool in improving the overall security posture of the .au DNS. For example, auDA requires all auDA accredited Registrars to comply with the Information Security Standard for Accredited Registrars. The registration rules operate as a barrier to entry into the .au domain for malicious actors or cyber criminals as there is a requirement that a person has an Australian nexus and that registrars verify registrant information prior to submitting an application for a domain name to the registry.[25]

Public Core of the Internet

17. The Domain Name System (DNS) is part of the Public Core of the Internet, which comprises the following layers:

(a) logical layer – applications, data and protocols that allow exchange of data, such TCP/IP, DNS and routing protocols

---

[18] Ibid[6.2.4]
[19] Ibid [6.3]
[20] Australian Government, Department of Communications and the Arts, Review of the .au Domain Administration (April 2018)
[21] Constitution of .au Domain Administration Limited, cl 1.2(b)
[22] Ibid cl 1.2(e)
[23] Ibid, cl 1.2d(iii)
[24] Ibid, cl 1.2(iv)
[25] 2012-04 Domain Name Eligibility and Allocation Policy Rules for the Open 2LDs, Schedule 1; 2012-05 Guidelines on the Interpretation of Policy Rules for Open 2LDs, para 6.

(b) Physical layer compromising the physical network components (hardware and other infrastructure such as telecommunication cables, Internet routers, DNS nameservers, and computers)

(c) Organizational layer such as internet exchanges, Computer Emergency Response Teams (CERTs), Registrars, Top Level Domain (TLD) Registries, TLD administrators and policy settings.

18. The Public Core of Internet only works properly if its underlying values of universality, interoperability and accessibility are guaranteed. In 2018, the 'five country' Ministers reaffirmed their vision of a "free, open, safe and secure internet."[26] Canada, United States of America, New Zealand, and Australia have not subscribed to the infrastructure in Internet governance approach adopted by other States, preferring to influence the behaviour of ccTLD administrators through non-legislative mechanisms.

Thematic Issues

Critical Infrastructure

19. auDA welcomes the Department's commitment to working with industry to identify and map assets and entities that may be critical infrastructure, including systems of national significance.[27] auDA provides these comments to assist the Department in forming a view as to whether auDA should be considered 'critical infrastructure' for the purposes of the proposed reforms and to assess the regulatory impact of these reforms on the operations of auDA as the .au ccTLD administrator.

20. DITRDC in its 2018 Review of .au Domain Administration did not go as far as identifying the .au ccTLD as critical infrastructure. DITRDC found that as auDA falls within the telecommunications sector which is a critical infrastructure sector under the Australian Government Critical Infrastructure and Resilience Strategy, it is therefore part of the critical infrastructure sector.[28] However, auDA is not subject to Part 14 of the *Telecommunications Act 1997* (Cth) (Telecommunication Sector Security Reforms).

21. auDA agrees that the .au DNS is critical infrastructure as defined in the Critical Infrastructure and Resilience Strategy,[29] as any disruption of the .au DNS may impact:

(a) the ability of critical infrastructure providers, businesses, non-government organizations and Australian governments to provide services and to communicate via the Internet; and

(b) users of these services wherever domiciled.

---

[26] Australian Government, Department of Home Affairs, Five country ministerial 2018 (accessed 18 September 2020) 1 <https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/five-country-ministerial-2018#:~:text=%20Five%20country%20ministerial%202018%20%201%20Official,spaces.%20We%2C%20the%20Homeland%20Security%2C%20Public...%20More%20>

[27] Australian Government, Department of Home Affairs, Protecting Critical Infrastructure and Systems of National Significance Consultation Paper (August 2020) 13.

[28] .Australian Government, Department of Communications and the Arts, Review of the .au Domain administration (April 2018) 14.

[29] Australian Government, Department of Home Affairs, Critical Infrastructure Resilience Strategy: Policy Statement (2015) 3.

However, the .au DNS is a network within a network. It is a system of globally distributed DNS nameservers and other infrastructure that is managed and operated by a range of parties, such as Registrars, Internet Service Providers, DNS service providers, website hosting companies, email service providers, and telecommunication providers. Its globally distributed nature raises significant issues in relation to Australian sovereignty over infrastructure outside its territorial borders.

22. auDA as the .au ccTLD administrator manages, either directly or through contracted service providers, only a small part of the overall DNS, auDA manages the:

    (a) .au top level zone

    (b) Registry database

    (c) Authoritative DNS nameservers

    (d) WHOIS registration data directory services (https://whois.auda.org.au/)

23. auDA accredits registrars to provide .au ccTLD domain name registration services, which often include DNS hosting. Registrars may also provide additional services such as webhosting and email. Registrars operate DNS infrastructure for the purposes of performing these functions. A significant proportion of auDA accredited registrars are domiciled overseas, and these registrars manage approximately two thirds of all .au ccTLD domains under management.

24. auDA has little visibility of other DNS Service Providers, such as ISPs, Webhosting companies, telecommunication providers and DNS providers (such as Cloudflare).[30] Webhosting, email service providers, and DNS providers are often domiciled overseas, such as Bluehost, Hostgator and Dreamhost.

25. The .au DNS has a large attack surface due to its globally distributed infrastructure network and .au DNS infrastructure operators. The proposed critical infrastructure reforms may create regulatory gaps due to jurisdictional issues that may make overseas auDA accredited registrars an attractive target for the purpose of espionage, sabotage and foreign interference targeting Australian critical infrastructure. The recent large-scale DNS hijacking campaigns demonstrate the national security risks of DNS compromise at the Registrar, ISP and telecommunication provider levels. Registrars and ISPs were targeted through spear phishing and other means to gain login details of DNS servers. The attackers then used these login details to change DNS server records to redirect user traffic to attacker-controlled infrastructure and to obtain valid encryption certificates for an organization's domain names, enabling man in the middle attacks.[31] The scale of these attacks against national security agencies and commercial enterprises in the Middle East was unprecedented.

[30] DNS Providers operate DNS network and software infrastructure, whereas DNS Service Providers are the businesses that you interact with to manage your online presence such as registering a domain name, accessing the Internet or hosting your website.

[31] Government of the United States of America, Department of Homeland Security, Alert (AA19-024A) DNS Hijacking Campaign (24 January 2019) https://us-cert.cisa.gov/ncas/alerts/AA19-024A; UK Government, National Cyber Security Centre, Advisory: Ongoing DNS hijacking and advice on how to mitigate (12 July 2019) https://www.ncsc.gov.uk/news/ongoing-dns-hijacking-and-mitigation-advice.

26. auDA would caution against categorizing .au DNS infrastructure as critical infrastructure and systems of national significance until the Department has time to complete a mapping exercise that (1) identifies .au DNS infrastructure and its location, (2) the operators of that infrastructure and (3) vulnerabilities within the .au DNS. auDA believes that the distributed nature of the .au DNS, and overseas infrastructure and operators may make any regulation less than optimal due to jurisdictional issues.

Current Regulatory Environment

27. The Australian Government has adopted a quasi-regulatory approach through the TOE for administering the .au ccTLD. The 2018 Review of the .au Domain Administration stated that the Australian Government "considers the TOE is an appropriate mechanism for Government in providing directions on its expectations of auDA."[32] This regulatory approach reflects the Australian Government's international position that no government should regulate the Internet, and that a multi-stakeholder model of internet governance is the most effective mechanism to develop public policy positions across the full spectrum of cyber affairs.[33] This multi-stakeholder internet governance model is reflected in the Australian Government's strong commitment to self-regulation of the .au DNS by the Australian Internet community.

28. auDA agrees that the TOE is the most appropriate mechanism through which the Australian Government should pursue its policy objectives, including ensuring the stable, secure and reliable operation of the .au domain space and responding quickly to matters that compromise DNS security.[34] The TOE have given auDA an authorizing environment in which to drive significant internal and external security reforms that aim to make the .au DNS stable, secure and resilient to a range of cyber incidents, insider threats, natural hazards and health emergencies.[35] The auDA Enterprise Security Strategy sets out all the measures that auDA takes to address security risks and robustness of its systems. [36]

29. auDA believes that transactional regulation is a more effective means of addressing security issues as it is not dependent on jurisdiction. The effectiveness of transactional regulation in addressing security risks in Registrar operated DNS infrastructure is demonstrated by the new Registrar Agreement, which will drive an uplift in the security posture of all auDA accredited Registrars. The new Registrar Agreement requires registrars to adopt and maintain an "Information Security Management System" in compliance with ISO27001 or another recognized standard as approved by auDA[37] and to implement and maintain the prescribed minimum security controls.[38] Registrars will be independently audited every 12

[32] Australian Government, Department of Communications and the Arts, Review of the .au Domain Administration (April 2018) 28.
[33] Australian Government, Department of Foreign Affairs and Australia's International Cyber Engagement Strategy (2016) https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/part_5_internet_governance_and_cooperation.html
[34] Australian Government, Department of Communications and the Arts, Review of the .au Domain Administration: Terms of Endorsement (issued 16 April 2018) 1<https://www.communications.gov.au/documents/review-au-domain-administration-terms-endorsement>
[35] auDA Enterprise Security Strategy https://www.auda.org.au/assets/Uploads/auDA-enterprise-security-strategy-.pdf
[36] auDA Enterprise Security Strategy https://www.auda.org.au/assets/Uploads/auDA-enterprise-security-strategy-.pdf
[37] Registrar Agreement, cl15.1
[38] Registrar Agreement, cl 15.3

months[39] and non-compliance will result in suspension from the Registry.[40] This means that Registrars will not be able to create any new domain name registrations. The Registrar Agreement also contains Personnel security requirements in respect to access to registry data.[41]

30. auDA has also been cognizant of the impact that any disruption or degradation of the .au DNS may have on Australian businesses, government, education and non-government organizations and users of these services. To address this issue, auDA has step in rights under the new Registrar Agreement, which enables it to assist the Registrar and Registry Operator should a Force Majeure event occur and there is a potential degradation or disruption to the .au DNS.[42]

31. The Cyber Security Strategy 2020 sets out a range of measures to keep Australians safe online. auDA plays an important role in ensuring that the .au ccTLD is not used by criminals and malicious actors to target Australians. auDA will be introducing a new Licensing Scheme that will require Registrars to validate the identity and Australian presence of a person applying for a domain name in the .au ccTLD,[43] new regulatory tools such as audit and domain name suspension powers and the Public Interest Test.[44] The Public Interest Test will allow an enforcement body or intelligence agency to request the deletion, suspension or to take other action in respect to a domain name where it is in the public interest.

32. auDA supports the Government's position that "Boards of critical infrastructure entities have visibility of, and are responsible for planning and actively managing security and resilience."[45] The auDA Board has established a range of governance measures to understand and advise on security risks. The Board receives detailed monthly operational reports on the key metrics associated with the .au DNS infrastructure, and receives reports of all incidents that impact the infrastructure. The Board's Security and Risk Committee (SRC) has responsibility for oversighting and advising the Board on matters relating to security and risk, including governance and risk management, security and business continuity. With respect to security, the SRC regularly monitors the integrity of auDA's security management against applicable policies and controls, and regularly monitors and reviews security enforcing functions including, activity monitoring, end-point protection software and processes, vulnerability and/or penetration testing, and DDoS mitigation to ensure they are fit for purpose and meeting the objective of applicable security policies.

33. The Board has also appointed an external Technical Advisory Standing Committee (TASC) to receive and consider input from the Internet technical community on aspects of auDA's operations, decisions or actions and provide advice to the Board. The committee comprises people with technical expertise in IP addressing, DNS, domain name registration operations, and IT security. auDA works closely with the Australian Signals Directorate

[39] Registrar Agreement, cl 16
[40] Registrar Agreement, cl 13.1
[41] Registrar Agreement, cl 15.5
[42] Registrar Agreement, cl 23
[43] Registrar Agreement, cl 21; .au Domain Administration Rules – Registrar, para 2.4; These new rules build on the existing requirements for registrars to verify a person's eligibility to hold a domain name under paragraph 6 of the *Guidelines on the Interpretation of Policy Rules for Open 2LDs* (2012-05).
[44] .au Domain Administration Rules – Licensing, para 2.17
[45] Australian Government, Department of Home Affairs, Protecting Critical Infrastructure and Systems of National Significance Consultation Paper (August 2020)

(ASD) to both seek its advice on security matters and offer assistance in identifying Australian systems that may have been comprised by malicious software. auDA actively participates in the activities of the Melbourne Joint Cyber Security Centre (JCSC), and, until the COVID-19 lockdown, had a staff member located at the JCSC to assist collaboration and information sharing with the Government and industry.

Regulatory reform

34. auDA has been through significant reforms over the last two years as a result of the 2018 Australian Government Review of the .au Domain Administration, including substantial uplifts in its security posture and reform of its Licensing Scheme to ensure that the .au is stable, secure and trusted. The Australian Government has reaffirmed its commitment to a self-regulatory regime for the .au ccTLD.

35. auDA is unclear as to what specific failings and weaknesses in the current arrangements that the Department would be seeking to address by capturing auDA as critical infrastructure under the proposed critical infrastructure reforms ('the CI reforms'). auDA believes that any deficit that may be identified by the Department in its security arrangements can be addressed through the TOE.

36. The upcoming DITRDC review of the TOE provides an opportunity for the Department to seek to incorporate the proposed security obligations in the TOE. The benefits of this approach, include:

    (a) maintains the Australian Government position that the internet should not be regulated by governments

    (b) consistent with the self-regulatory model for administering the .au ccTLD

    (c) overcomes jurisdictional issues as auDA can use its contractual arrangements to implement the obligations across its Registrars

    (d) harnesses the role of auDA to develop and enforce policies

    (e) develops industry wide solutions to security issues

37. In the event, that this quasi-regulatory approach does not achieve the desired public policy outcomes, then the Department still has the option of:

    (a) prescribing or declaring the .au ccTLD or parts of the .au DNS as a critical infrastructure asset under section 9(1)(f) or section 51 of the *Security of Critical Infrastructure Act 2018* (Cth) ('SOCI Act') or

    (b) declare auDA as a carriage service provider for the purposes of Part 14 of the *Telecommunications Act 1997* (Cth).

38. auDA firmly believes that regulation under the SOCI Act or *Telecommunications Act 1997* (Cth) should be a last resort option due to the regulatory burden that this would place on auDA as a not for profit organization. The Australian Government recognizes that

regulation may have a disproportionate impact on not for profits compared with commercial organizations.[46]

39. auDA is a relatively small organization with a staff of 25 FTE, which are spread across its technical, corporate, and regulatory and enforcement functions. It is self-funded through the wholesale proportion of the registration fee that a person pays to a registrar when registering a domain name. This wholesale fee is shared with the Registry operator. auDA would need to employ additional staff to meet its obligations under the SOCI Act or *Telecommunications Act 1997* (Cth) to avoid having to reallocate staff from essential functions, such as compliance and enforcement, and recover the costs through increases in the wholesale licence fee.

Critical Infrastructure Reforms

Industry – Government Collaboration

40. auDA agrees that industry and government collaboration is essential to achieving an uplift in security standards across multiple critical infrastructure sectors through principles-based regulation, which provides operators with the necessary agility to respond to a rapidly evolving security and threat environment. auDA welcomes the introduction of a range of measures that will improve collaboration, such as industry-government secondment program, threat assessments and briefings. auDA has found that having an outposted compliance officer in the Melbourne Joint Cyber Security Centre has provided a range of benefits, including enabling a better understanding of the government's cyber security approach and processes, and increased collaboration and information sharing with other industry sectors.

Principles based outcomes

41. The Government's principles-based outcomes approach is welcome as it recognizes that critical infrastructure owners and operators are better placed to determine what processes and actions are required within their business to achieve the desired outcome. As a not for profit, auDA welcomes the flexibility to choose the most appropriate and cost-effective way of achieving any regulatory obligations.

42. The principle based outcomes that require an entity to (1) understand risks, (2) mitigate risks to present incidents, (3) minimize the impact of realized incidents and (4) effective governance and high level security obligations relating to physical, cyber, personnel and supply chain security appear to be reasonable, and appropriate response to an all hazard approach to critical infrastructure protection.

43. While supportive of principles-based regulation, auDA is concerned that to be an effective form of legislation that it will need to be supplemented by detailed regulations, standards, and guidelines. The Government has committed to working with industry to co-design sector specific standards that are proportionate to risk in respect of the positive security obligations. auDA welcomes this commitment and would encourage the Department to establish Implementation Working Groups across all sectors. However, there is no detail in the Consultation paper as to the regulation and rule making powers. auDA notes that the Minister has a broad rule making power under section 61 of the SOCI Act, which includes

[46] Australian Government, Department of Prime Minister and Cabinet, Office of Best Practice Regulation, Community organisations (March 2020)

"the making of rules necessary or convenient to be prescribed for carrying out or giving effect to the Act." auDA is concerned that the regulation and rule making powers may lead to regulatory creep and strongly advocates for legislative criteria that restrict the matters for which these powers can be used.

Enhanced Cyber Security Obligations

44. auDA is concerned about the lack of transparency in respect to the Enhanced Cyber Security Obligations, which appear to be a significant expansion of national security agencies' powers. auDA acknowledges that the high level description of these powers means that any comments are a 'stab in the dark' as to the operation and implication of the Enhanced Security Obligations.

Systems of National Significance

45. auDA notes that the Enhanced Cyber Security Obligations will only apply to systems of national significance. The Consultation paper does not define a system of national significance but lists two factors that will be considered (1) interdependency with other functions and (2) consequence of the compromise. Arguably, the .au DNS is a system of national significance as critical infrastructure operators, governments, education service providers, businesses and non-government organizations rely on it to provide services via the Internet and for communication. Any disruption of the .au DNS depending on the level targeted within the .au ccTLD hierarchy will have a significant impact on service providers and the broader Australian community.

46. The criteria for determining what is a system of national significance are extremely broad and subjective, given the nature of the Enhanced Cyber Security Obligations. auDA recommends that any definition contains threshold requirements and safeguards to prevent scope creep. Government should be required to consult with a critical infrastructure owner and operator before an asset can be declared a system of national significance, and any declaration should be subject to challenge by the asset owner or operator and subject to scrutiny by an appropriate oversight body.

Situational awareness

47. auDA supports the Australian Government proposal to improve owners and operators' planning and preparedness against cyberattacks. auDA supports in principle information sharing with Government for the purpose of establishing a 'near real time threat picture' but is concerned about the potential blurring of the boundary between threat intelligence and surveillance. auDA seeks further clarity on:

    (a) who in Government can issue a request for information,

    (b) the time frames for responding to a request

    (c) the time frame a request can be in force (i.e. 6 months or ongoing)

    (d) rules governing disclosure and information sharing and information retention

48. auDA is also cognizant that there are significant jurisdictional issues that may arise from collecting and using data from its global network of .au DNS nameservers. The majority of .au nameserver traffic originates from overseas, and the privacy and data implications which may arise warrant careful consideration.

Directions and Direct Action

49. The Cyber Security Strategy 2020 states that "in consultation with critical infrastructure owners and operators, Government will develop new powers proportionate to the consequences of a sophisticated and catastrophic cyberattack, accompanied by appropriate safeguards and oversight.' However, the Consultation paper only provides a high level summary of the proposed directions and direct action powers, making it difficult to grasp how these powers will work, who in Government will exercise these powers, and what, if any, accountability and transparency mechanisms will apply.

50. The directions power will be enlivened where there is an imminent cyber threat or incident that could significantly impact Australia's economy, security or sovereignty and the threat is within the capacity of the critical infrastructure operator to address. The Government can provide reasonable, proportionate and time-sensitive directions to entities to ensure action is taken to minimize its impact. Based on this description, the proposed Ministerial directions power appears to remove the thresholds and safeguards in the existing Ministerial directions powers under section 32 of the SOCI Act or section 315B(2) of the *Telecommunications Act 1997* (Cth). It is unclear why a new directions power is needed.

51. auDA strongly advocates that the proposed directions power be subject to stringent issuing criteria, including a requirement to negotiate or consult with a critical infrastructure operator in good faith. auDA believes that critical infrastructure operators are best placed to understand the nature of the threat, and its impact on their systems and customers and appropriate mitigation strategies.

52. The Consultation paper has not provided sufficient detail to understand how the direct action power would work, except that in an emergency the Government could take direct action to defend and protect the network and systems of critical infrastructure entities and systems of national significance. It is not clear if the direct actions power would allow the Government to act in anticipatory self defence.

53. auDA welcomes the Government's advice that these powers will be "accompanied by appropriate safeguards and oversight. As there is no detail as to what these safeguards and oversight mechanisms may be, auDA suggests consideration be given to:

    (a) conferring an authorisation power on the Court

    (b) right to appeal a decision relating to a request for information and directions

    (c) administrative oversight by the Inspector-General of Intelligence and Security where the authority is an intelligence agency

    (d) periodic review of the directions and direct action powers by the Parliamentary Joint Committee on Intelligence and Security.

Consultation

54. auDA believes that the Consultation paper is too abstract to really understand the obligations being proposed by Government and how they will impact on the operations of auDA as the administrator of the .au ccTLD and other DNS infrastructure providers. auDA is particularly concerned about the directions and direct actions power, and the legal immunities that may attach to the actions of government when 'it all goes wrong'.

55. auDA welcomes the Department's advice that it will be provided with an Exposure Draft of the Bill and given an opportunity to comment. However, auDA is concerned that given the legislative time-line presented at the workshops, that there will be insufficient time for genuine and considered consultation. auDA would welcome any opportunity to participate in any implementation working groups for the telecommunications sector.

ATTACHMENT A

Domain Name System

Overview

The DNS is a distributed hierarchical database which contains a listing of domain names and various types of information about them. A domain name denotes an Internet Resource such as a website, an email server, a database server or any machine or service that is connected to the internet. Although the DNS has a variety of uses, the most important function of the DNS is to associate domain names with Internet Protocol (IP) addresses of the systems that host the Internet Resource. This allows users to access Internet Resources using memorable and recognizable names. The DNS creates a logical linkage between the domain name and Internet Resource, which ensures that the domain name stays the same even though the IP address of the host of that Internet Resource may change.

.au structure

The .au ccTLD is the Australian address book for Australian licensed domain names in the DNS hierarchy. The Internet Resources referenced by these domain names, such as websites, email servers, database servers, and any device connected to the Internet, can be and frequently are located outside of Australia. For example it is very common for Australians to host their websites in the USA, to take advantage of lower cost Internet capacity . The .au ccTLD is a hierarchically organized tree structure. The .au domain branches into special purpose second level domains (2LD), and the edu.au 2LD and the gov.au 2LD branch into third level domains (3LD) representing each State and Territory (Fig 1).

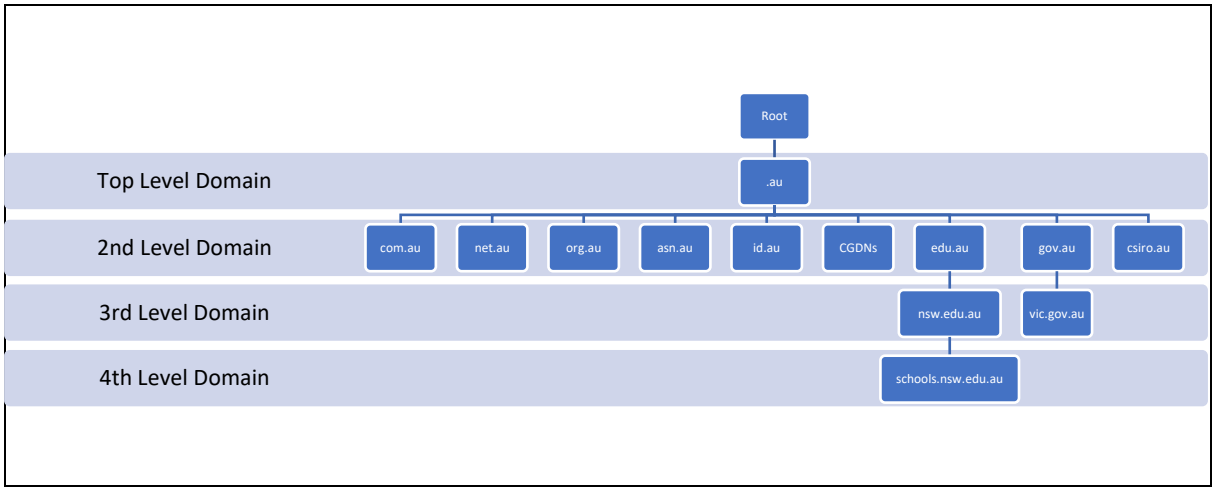


Figure 1: Structure of the .au ccTLD

Each 2LD and 3LD has a special purpose, which makes it easier for a person to identify the type of entity using the domain name and reduces consumer search costs (Table 1). The 2LDs are further categorized into:

(a) open 2LDs (com.au, net.au, org.au, asn.au and id.au) which allow any person to register a domain name, subject to satisfying the eligibility and allocation criteria for that 2LD.

(b) restrictive 2LDs are the State and Territory namespaces (vic.au, nsw.au, sa.au, tas.au, act.au, qld.au, nt.au and wa.au). Registration of domain names in the State and Territory 2LDs are restricted to community groups within the border of the

State or Territory to which the 2LD corresponds. The domain name used by the community must match the name of the geographical locale in which the community group resides.

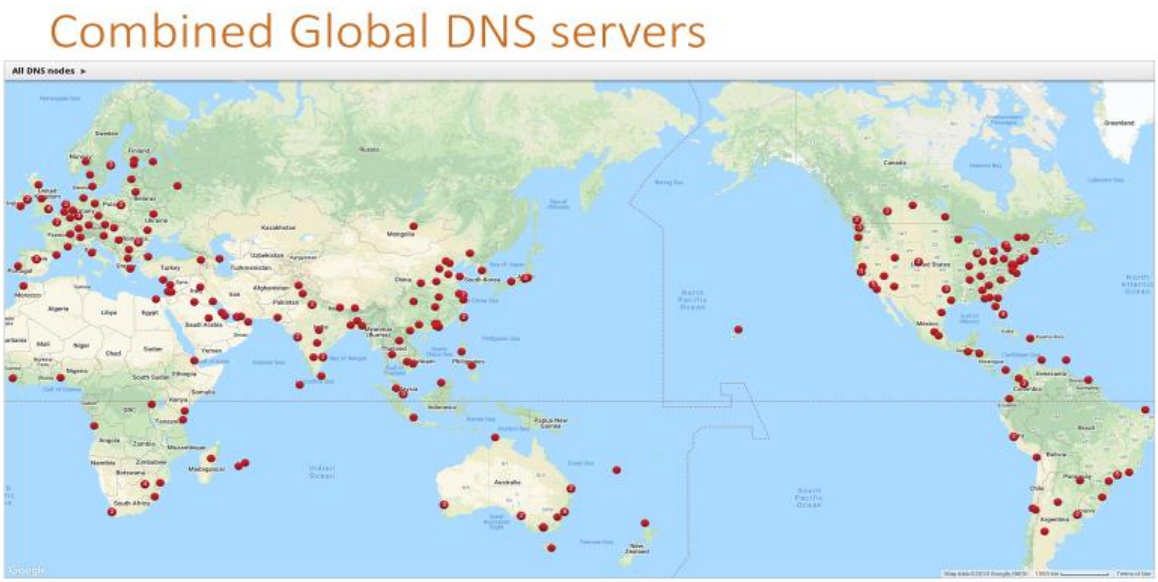
(c) closed 2LDs are the gov.au and edu.au 2LDs.

The gov.au 2LD comprises the State and Territory Government 3LDs (vic.gov.au, nsw.gov.au, qld.gov.au, nt.gov.au, wa.gov.au, sa.gov.au, act.gov.au and tas.gov.au). auDA has delegated administration of the gov.au 2LD and child zones to the Australian Government Digital Transformation Agency under the gov.au Sub-Sponsorship Agreement.

The edu.au zone comprises the State and Territory education 3LDs. A person can only register a domain name in the edu.au 2LD or State or Territory 3LD if it is a regulated education provider or a related service provider, such as university colleges. For example, all Victorian Government primary and secondary schools have their domain name registered in the vic.edu.au 3LD.

All domain names registered in the 2LDs and 3LDs are recorded in the Registry, except domains within csiro.au, and the tas.gov.au and nt.gov.au 3LD. These domains are managed by third party administrators, and the csiro.au, tas.gov.au and nt.gov.au domains in the Registry only contain a pointer to DNS nameservers that contain information about the sub-domains in these 3LDs.

The .au DNS database is distributed across a very large number of geographically dispersed DNS nameservers that are managed by auDA or by contracted third party providers (Map 1).



Map 1: Global .au DNS servers

Each DNS nameserver contains information relating to a subset of the DNS namespace and pointers to other nameservers that can point to other parts of the data base. For example, a gov.au nameserver will point to the vic.gov.au nameservers, which will point to the police.vic.gov.au nameservers, which will provide the IP addresses for the website and email servers associated with the domain name police.vic.gov.au.

DNS queries

A person will type a domain name (auda.org.au) into a web browser, the query will be sent to the local DNS resolver in the person's computer. If the DNS resolver has a locally cached copy of the domain name's IP address, then it passes the information back to the browser. However, if there is no cached record, then the computer will ask a DNS resolver for the domain name's IP address. The DNS resolver starts by querying a root DNS server for the IP addresses of the .au TLD nameservers. The DNS resolver will then ask a .au TLD DNS nameserver for the IP addresses of the org.au DNS nameservers. The DNS resolver will then ask an org.au DNS nameserver for the IP addresses of the auda.org.au DNS nameservers. Finally the DNS resolver will ask an auda.org.au DNS nameserver for the IP address of the www.auda.org.au web server, and passes it back to the browser, which then contacts the website host using the IP address (Fig 2).

DNS Service Providers

There are several parties that are involved in providing DNS services. The DNS database is maintained by the Registry operator. auDA outsources the .au Registry function to Afilias Australia Pty Ltd, who is contracted to provide registration services for registrars, authoritative DNS nameserver services, the WHOIS registration data directory services and registrar support services for the .au ccTLD.

A person cannot register a domain name directly with the Registry and must use an auDA Accredited Registrar. Registrars are required to meet the auDA Information Standard (ISS) for Accredited Registrars and pass an independent audit before they become an auDA accredited Registrar and are granted access to the Registry. auDA as part of the reforms of the .au Licensing Framework requires Registrars to adopt and maintain an effective "Information Security Management System" in compliance with ISO 27001 or adopt and maintain any other recognized framework or standard approved by auDA.[47] auDA also requires Registrars to implement prescribed minimum security controls,[48] which are based on the Australian Signals Directorate Essential Eight.

Internet Service Providers (ISPs) provide DNS resolution services to their subscribers to enable them to use the DNS system and Internet. ISP customers are reliant on whatever recursive DNS resolvers the ISP uses for basic internet connectivity, and loss of the recursive DNS server can cut off nearly all Internet access for ISP subscribers. An ISP customer is free to use another DNS resolver of their choice (e.g. Cloudflare and Google public DNS resolvers) at no charge, but few customers know how to change the default configuration of their software. On 2 August 2020, several Telstra nameservers failed to resolve leaving some Telstra customers without Internet access. [49]

[47] auDA Registrar Agreement, cl 15.1(b)(ii)-(iii) < https://www.auda.org.au/assets/Uploads/auDA-Registrar-Agreement-20200625.pdf>
[48] Ibid, cl15.3
[49] Sydney Morning Herald, Telstra backtracks on claim network was hit by cyber attack (2 August 2020)

1) Laptop asks Resolver (ISP/Corporate/Personal) "where is www.auda.org.au"
2) Resolver takes on the job and asks the root server "where is www.auda.org.au"
3) Root server responds "I don't know but I do know where .au is, go ask them and here is their IP address"
4) Resolver asks the .au Name Server "where is www.auda.org.au"
5) The .au Name Server responds "I don't know but I do know where org.au is, go ask them and here is their IP address"
6) Resolver asks the org.au Name Server "where is www.auda.org.au"
7)The org.au Name Server responds "I don't know but I do know where auda.org.au is, go ask them and here is their IP address"
8) Resolver asks the auda.org.au Name Server "where is www.auda.org.au"
9) The auda.org.au Name Server response "I know, its at 104.17.237.107"
10) Resolver passes the IP for www.auda.org.au back to the laptop
11) Laptop talks directly to the webserver via the IP address
12) The auda.org.au webserver responds directly to the end user laptop with the page requests

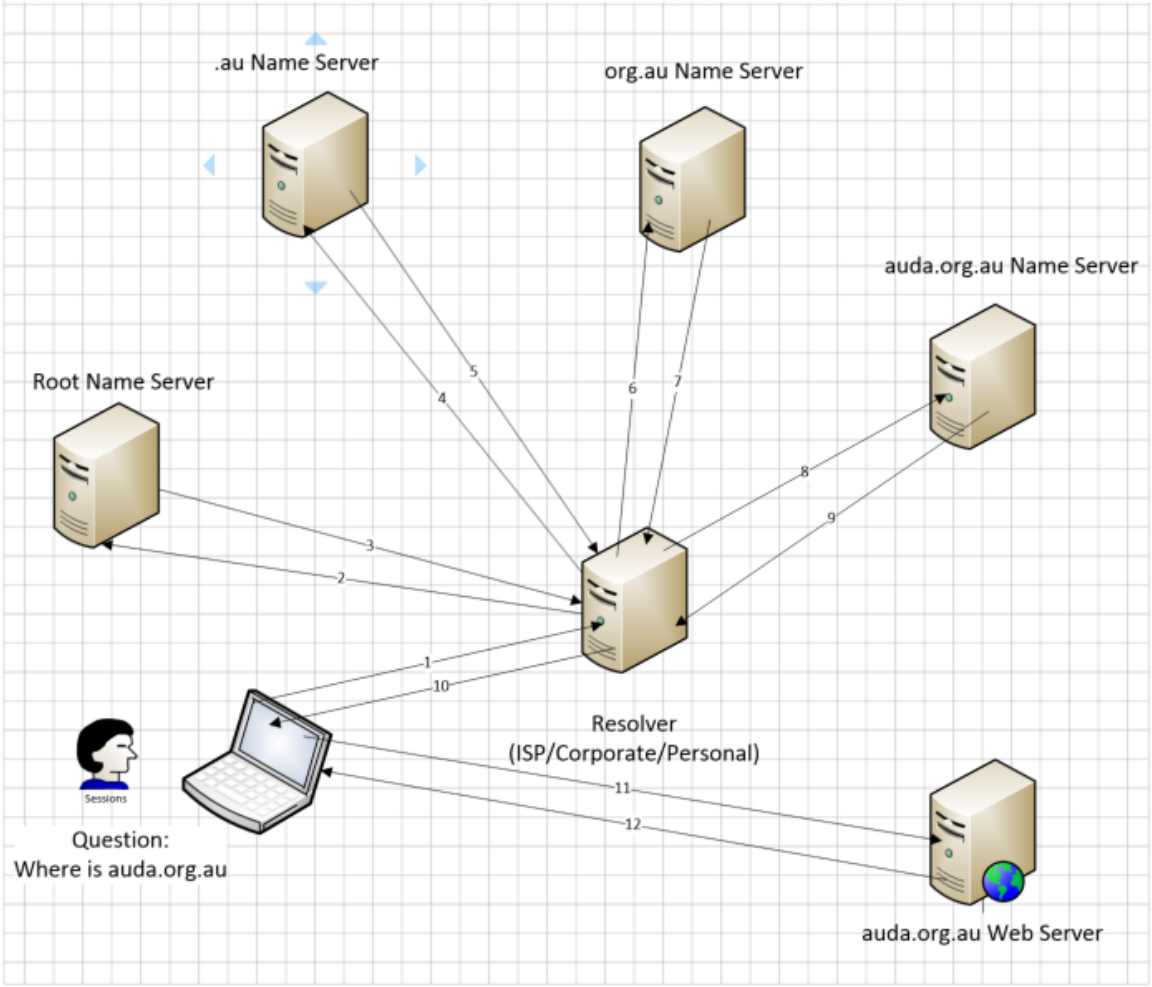


Figure 2: DNS queries

As the DNS is a network within a network, it relies on other internet and communications infrastructure, such as Internet Exchange Points, land based optical fibre, and submarine cables.

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.

28.

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

[14] Ibid, s17(2)(b)

Positive Security Obligations

29. 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

30. 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]

31. 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]

32. 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

33. 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.

34. 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

[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]

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 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

35. 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]

36. 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

37. 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

[22] Ibid 50[319]

[23] Ibid

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

imposition of additional security obligations (Enhanced Security Obligations), including system information gathering notices.

38. 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]

39. 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.

40. 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.

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

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

Access to systems information

41. 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 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

42. 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

43. auDA has significant reservations about the authorisation framework for the exercise of powers under 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).

44. 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

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

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 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.

45. 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.

46. 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.

---

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

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

Last resort powers

47. 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.

48. 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.

49. 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

[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)

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

50. 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.

51. 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