March 2022

Submission to the Parliamentary Joint Committee on Intelligence and Security

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

.auDA

Introduction

auDA

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 an agreement with the Internet Corporation for Assigned Names and Numbers (ICANN) to manage the .au ccTLD and operates under Terms of Endorsement issued by the Australian Government which require auDA to manage the .au domain in the public interest.

As a critical part of the digital economy, our purpose is to provide a safe, secure, and reliable namespace for the benefit of all Australians.

auDA performs the following functions:

- develop and implement domain name policy
- license 2LD registry operators
- accredit and license registrars
- implement consumer safeguards
- facilitate .au Dispute Resolution Policy
- represent .au at ICANN and other international fora
- technical management of the .au zone file
- manage and maintain a secure and stable Domain Name System.

auDA operates under an industry self-regulatory model, working closely with suppliers, business users, non-profit organisations, consumers and the Australian Government.

It seeks to serve the interests of the Internet community as a whole and takes a multi-stakeholder approach to Internet governance, where all interested parties can have their say.

Advocacy

auDA's advocacy is guided by the following key principles:

1. **Purpose driven** – we are a for purpose organisation. Our purpose is to:
    a. administer a trusted .au domain for the benefit of all Australians
    b. champion an open, free, secure and global internet

2. **Multi-stakeholder Approach** - we take a multi-stakeholder approach to our work, working closely with domain name suppliers, businesses, not-for-profit organisations, education and training providers, consumers and Government entities to serve the interests of the Internet community as a whole.
3. **Independence -** we are independent from government and operate transparently and openly in the interests of all Australians
4. **Leadership** – we seek to actively advance an open, free, secure and global internet and positively influence policy and outcomes related to internet governance, including through undertaking research and informing and educating Australians about an open, free, secure and global internet and its benefits
5. **Support the digital economy through innovation and partnership** – we seek to partner with like-minded organisations and foster innovation across the technology sector, recognising its benefit to growing our digital economy and, in turn, benefitting of all Australians. We recognise the impact that legislative burden can have on innovation in the technology sector and encourage a consultative approach to regulation.

auDA's work in administering Australia's domain name infrastructure is undertaken through a multi-stakeholder approach and in partnership with others for the benefit of all Australians. We understand the criticality of the .au domain name system (DNS) infrastructure to the social and economic lives of Australians and the heightened need for a risk-based approach to cybersecurity given this dependence. It is in this vein that we offer comment on the *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022.*

Submission

As noted before the PCIS in the past , auDA supports the Government's policy objectives to protect and defend Australia's critical infrastructure. The .au ccTLD is undeniably part of Australia's critical infrastructure as it supports the stable, reliable and secure operation of the DNS in Australia. The DNS enables internet users to connect to information (websites) and people (email) for information and services.

This fact is now recognised in the *Security of Critical Infrastructure Act 2018* amendments that received Royal Assent in December 2021. Furthermore, auDA is prescribed as the relevant entity critical to the administration of an Australian domain

[1] auDA subm ss on to PJC S on Secur ty Leg s at on Amendment (Cr t ca nfrastructure) B 2020

name system in Section 16 of the *Security of Critical Infrastructure (Definitions) Rules 2021*.

auDA has engaged with the Department of Home Affairs throughout the critical infrastructure reform consultation process through submissions, town hall meetings and meetings with departmental staff. We also provided a submission to the Committee and appeared as a witness on 8 July 2021.

We welcome this opportunity to provide further input to the Committee on the Exposure Draft of the *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022* and offer the following comments:

1. Part 2A Critical infrastructure risk management programs

auDA takes seriously its responsibility to manage risk related to management of critical infrastructure and has developed and implemented a robust risk management program. auDA complies with the ISO 31000 standard related to risk management, the ISO 27001 standard related to Information Security Management Systems and adheres to the Australian Cyber Security Centre's Essential Eight Maturity Model. auDA's risk management program is approved and regularly reviewed by our Board and its Security and Risk sub-committee, and its ISO 27001 system is externally reviewed by independent auditors annually

The Explanatory Document acknowledges that bringing business practices into line with the risk management obligations may take time and that certainty about requirements in the rules is necessary. auDA agrees that the rules should allow a minimum of 6-month delayed commencement to allow an appropriate transition period and also provide additional time for businesses to comply with specific obligations within their Risk Management Programmes. This should be reflected in the Bill to provide certainty that rules made for the purpose of section 30AB will not take effect for a period of at least 6 months from when the rules are made.

We also consider that section 30AH(6) should be amended to include that the Minister must have regard to input from entities responsible for critical infrastructure assets in specifying the requirements in the rules made for the purposes of paragraph (1)(c) to ensure they are fit for purpose.

2. Part 2C Enhanced cyber security obligations

The Explanatory Document to the exposure draft notes that the enhanced cyber security obligations will be considered on a case-by-case basis, following consultation with the entity.

auDA already has in place incident response plans, prepared in accordance with relevant ISO standards, conducts annual vulnerability assessments and the results are reported to the Board and shared with the Government's representative on the Board, and undertakes regular cyber security exercises.

We consider that the Bill should be amended so that the Secretary is required to consult with an entity for a minimum of 28 days before the enhanced cyber security obligations are applied, and that the Secretary must have regard to any input provided by entities during this consultation. This would ensure the Secretary understands the nature of the entity's asset and the security arrangements already in place, reducing the possibility that obligations are duplicative or not fit for purpose.

2.1 Division 5 Access to system information

auDA is concerned that the provisions in Division 5 relating to access to system information lack specificity. Furthermore, they allow the Secretary to exercise broad discretion, with the only requirements being consultation with the operator of a critical Infrastructure asset, and that the information is not personal Information (within the meaning of the *Privacy Act 1988*).

We are also concerned that section 30DJ provides for the Secretary to require installation of system information software on a computer needed to operate a system of national significance if the Secretary believes on reasonable grounds that a relevant entity would not be technically capable of preparing reports on systems information. Even if there are reasonable grounds for considering that a relevant entity would not be technically capable of preparing reports on systems information, the installation of software in an existing, highly critical environment that has been subject to extensive testing may cause unexpected and untested side effects and should be avoided.

As noted in our February 2021 submission to the Committee[2] and our November 2020 submission to Home Affairs[3], 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. In *the Privacy Commission v Telstra Corporation Limited (2017) FCAFC 4*, the court found that metadata is personal information when it is about an individual.

Furthermore, we reiterate that DNS data not only captures data relating to Australians but also to foreign entities and individuals, whose information (including metadata)

---

[2] auDA subm ss on to PJC S on Secur ty Leg s at on Amendment (Cr t ca nfrastructure) B 2020 para 32
[3] auDA subm ss on to DoHA on the Exposure Draft of the Secur ty Leg s at on Amendment (Cr t ca nfrastructure) B 2020 para 40

may be protected under laws with extraterritoriality, such as the General Data Protection Regulation. Accordingly, this provision may force organisations such as auDA to breach these laws and face the consequences of such a breach.

In our opening statement to the 8 July Committee hearing and also our submission to Home Affairs,[4] we stated that the use of powers to compel the provision of system information from computers used to operate a system of national significance should only be authorised by a judicial officer. This remains our position as it would provide a greater degree of independence and rigour to the process, and would be consistent with the exercise of other coercive powers such as the *Regulatory Powers (Standard Provisions) Act 2014* (Cth), and the *Crimes Act 1914 (Cth).*

With respect to invoking the powers of provision 30DJ, where the Secretary may require installation of system information software, we refer to our previous submission[5] and continue to advocate for a statutory requirement for government to state consultation has been undertaken with the relevant entity, and any concerns or issues expressed by the entity have been taken into account.

3. Part 6A Declaration of systems of national significance

We note that under 52C the Minister will invite an entity to make a submission before declaring an asset a system of national significance. While a period of consultation is welcome, auDA considers 28 days (or a shorter period if specified) may be too short, particularly given the highly specialised nature of the assets being considered and, in auDA's case, the international nature of the DNS. auDA suggests the Bill be amended to allow for a longer consultation period of at least 45 days.

We also suggest that section 52B(2) be amended so that any submission made by an entity in response to a proposed declaration is included in the matters the Minister must have regard to in determining whether an asset is of national significance.

4. Regulation Impact Statement and Statutory Review

We note that it is proposed the Bill be enacted without a final Regulation Impact Statement. This is a concerning deviation from best practice regulatory design. Given the Bill imposes obligations on industry without an option for cost recovery, the Regulation Impact Statement should not be overlooked for the sake of expediency.

[4] auDA open ng statement to PCJ S hear ng 8 Ju y 2021 and auDA subm ss on to DoHA para42
[5] auDA subm ss on to DoHA para 47

Additionally, section 60B of the *Security of Critical Infrastructure Act 2018* provides that the Committee may review the operation, effectiveness and implications of the Act within 3 years of receiving Royal Assent. Given the broad application of the legislation across multiple sectors, the lack of specificity in this Bill and the absence of a Regulation Impact Statement (unless this latter point is reconsidered), auDA recommends that such a review be required.

In conclusion, the prevention of cyber-attack and rapid response in defending Australia's critical infrastructure is vitally important and we appreciate the opportunity to engage with government on this issue. To this end, we would be pleased to meet with the Committee and speak to our submission or provide additional information should the Committee seek it. The contact officer for this matter is Annaliese Williams, Policy Adviser, who may be contacted at [redacted]

Yours sincerely,

[redacted]

Rosemary Sinclair AM

Chief Executive Officer