Submission to the Department of Home Affairs:

Cyber Security Legislative Reforms Consultation

February 2024

.auDA

Contents

Contents **2**

Introduction **3**

Who is auDA? 3

auDA's role 3

auDA's stakeholders 3

auDA's advocacy principles 4

Submission **5**

PART ONE: New cyber security legislation 5

Measure 2: Ransomware reporting obligation for businesses 5

Measure 3: Limited use obligation on the Australian Signals Directorate and the National Cyber Security Coordinator for information provided during a cyber attack 6

Measure 4: Cyber Incident Review Board 7

PART TWO: Amendments to the Security of Critical Infrastructure Act 2018 8

Measure 5: Protecting critical infrastructure - data storage systems and business critical data 8

Measure 6: Consequence management powers 8

Measure 7: Protected information provisions 9

Measure 8: Review and remedy powers 9

Summary **10**

Introduction

Who is auDA?

.au Domain Administration Ltd ("auDA") is the administrator of the .au country code Top Level Domain (ccTLD). The .au ccTLD includes the following namespaces: .au, com.au, net.au, org.au, asn.au, id.au, vic.au, nsw.au, qld.au, sa.au, tas.au, wa.au, nt.au, act.au, edu.au, gov.au.

auDA's role

As a critical part of the digital economy, auDA's role is to ensure the .au ccTLD remains stable, reliable and secure. Additionally, auDA performs the following functions:

- Administers a licensing regime for .au domain names based in multi-stakeholder processes, including managing enquiries and maintaining an appropriate compliance and dispute resolution processes associated with the licensing rules
- Appoints the .au registry operator and accredits .au registrars
- Advocates for, and actively participates in, multi-stakeholder internet governance processes both domestically and internationally.

auDA's stakeholders

In performing its functions, auDA operates under a multi-stakeholder model, working closely with suppliers, business users, industry, civil society, consumers, academia, the technical community and the Australian Government.

auDA 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.

auDA is part of a global community of organisations in the domain name industry and engaged in internet governance. It plays an active role in representing .au at international fora, such as the Internet Corporation for Assigned Names and Numbers (ICANN), the Asia Pacific Top Level Domain Association (APTLD), as well as global and regional Internet Governance Forums (IGFs).

auDA was proud to host the 2023 Asia Pacific Regional IGF in Brisbane from 29-31 August, as well as other key events taking place alongside: the Pacific IGF, the Asia Pacific Youth IGF and Australia's national IGF, NetThing. This year, we are pleased to sponsor the Internet Engineering Task Force, which is being held in Australia for the first time from 16-22 March in Brisbane.

auDA's advocacy principles

auDA's local and international advocacy is undertaken in accordance with the following key principles:

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

    Our purpose serves our vision, which is to unlock positive social and economic value for Australians through an open, free secure and global internet.
2. **Multi-stakeholder approach** - We take a multi-stakeholder approach to our work, and we advocate for multi-stakeholder approaches to internet governance and policy matters. This involves us working closely with domain industry and other technical community stakeholders, businesses, not-for-profit organisations, education and training providers, consumers, and Government entities to serve the interests of the internet community as a whole.
   This approach is founded on strong relationships locally and globally.
3. **Independence** - We are independent from government and from the corporate sector. We operate transparently and openly in the interests of all Australians.
4. **Leadership** – We seek to lead Australia's internet community to work better together on our shared work to actively advance an open, free, secure and global internet and positively influence policy and outcomes related to internet governance.
   We do this through quality policy advice and analysis, through research and information, and by sharing this insight with those who can benefit from it. Partnership is integral to our way of working – we seek to work with others in Australia, as well as regionally and globally, who support our vision and can help multiply our impact.
5. **Encouraging innovation** – We support an innovative digital economy, and through our work we foster innovation across the technology sector, recognising its benefit to growing our digital economy and, in turn, benefitting all Australians.
   In the technology sector where innovation is rapid, we encourage the use of incentives and self-regulation where possible, and advocate for a consultative multi-stakeholder approach to legislation and regulation where it is needed.

Submission

auDA supports the Australian Government's objective to uplift Australia's cyber security as set out in the *Australian Cyber Security Strategy 2023-30.* We acknowledge the willingness of the Department of Home Affairs to engage with industry during consultation on the proposed cyber security legislative reforms and welcome the opportunity to participate in roundtables and town hall meetings. We are pleased to offer the following comments on the measures proposed in the *Cyber Security Legislative Reforms Consultation Paper.*

PART ONE: New cyber security legislation

Measure 2: Ransomware reporting obligation for businesses

Ransomware is a significant threat to Australian businesses and individuals and auDA supports the policy objective of establishing a reporting obligation to increase visibility of the extent of ransomware attacks. Better understanding of the type and scale of attacks will assist both government and the private sector to prepare for and defend against these in the future and we support regular public sharing of anonymised information.

In principle, we support the proposed no-fault, no-liability approach. Since the policy intent is risk mitigation and prevention of future attacks, we believe the focus should be on education and establishing a community expectation that ransomware incidents should be reported, rather than penalising victims of attacks.

We consider the thresholds for determining what constitutes a reportable incident require careful consideration and should be set out in the legislation. We also consider that the relationship between this measure and the limited use obligation in Measure 3 should be clarified.

Who should be subject to reporting obligations?

auDA acknowledges the rationale of limiting the scope of the proposed obligation to entities with a turnover above $10 million and we agree that the burden on small business must be balanced against the value of the information obtained via a mandatory reporting framework.

However, we note that small businesses represent a significant proportion of the Australian economy and exempting them from the obligation may result not only in many attacks going unreported, but it may also make them a more attractive target for malicious actors. A targeted ongoing education campaign may help small business better understand how to mitigate risks and encourage voluntary reporting of attacks. auDA requires all staff and Board to complete monthly cybersecurity training.

There may be benefit in considering a risk-based approach to the mandatory obligation as opposed to size. For example, many small businesses are suppliers to critical infrastructure operators, and it may be appropriate for these businesses to report ransomware attacks as part of managing supply chain risks.

Additionally, some small businesses routinely handle sensitive information, as defined in the *Privacy Act 1988* (Privacy Act). A ransom or cyber extortion attack on these businesses could have significant consequences for the community. It may be appropriate to consider extending the reporting obligation to any businesses subject to the Australian Privacy Principles.

Relationship to existing reporting obligations

We agree that where an entity is subject to an existing reporting obligation, any new ransomware reporting obligations should form part of that. For example, entities subject to the *Security of Critical Infrastructure Act 2018* (SOCI Act) reporting obligations should report under that framework in preference to creating an additional reporting framework.

Measure 3: Limited use obligation on the Australian Signals Directorate and the National Cyber Security Coordinator for information provided during a cyber attack

The Consultation Paper acknowledges that industry stakeholders are increasingly reluctant to share detailed cyber incident information with government and that cyber incident reporting has remained steady despite an increase in cyber incidents across the economy.

auDA understands that industry stakeholders have previously requested safe harbour provisions for data provided to government during a cyber incident to protect against legal liability resulting from a cyber incident, and that this is not being considered.

We note the proposed limited use obligation would not preclude information provided to the Australian Signals Directorate and/or the National Cyber Security Coordinator being shared with other government agencies, including law enforcement and intelligence agencies and regulators for "cyber security purposes". While we recognise that a regulator may use existing powers to compel an entity to provide information, we consider that the permitted uses within "cyber security purposes" should explicitly exclude regulatory or compliance action.

We also suggest clarification of how an entity's commercial or other interests could be protected where information is provided for cyber security purposes (e.g. Freedom of Information exemptions etc.).

Overall, we consider this measure as it is currently proposed is unlikely to reduce any existing hesitation to share detailed information and will do little to achieve the objective of promoting open engagement with already-reluctant stakeholders. We believe open engagement should continue to be the goal and suggest that further work be done on this measure to reflect that goal.

The Consultation Paper notes that low industry engagement with government agencies may be driven by a shift to a more compliance-based approach. auDA suggests a renewed focus on cooperation and collaboration between government and industry, and building trust through two-way information exchange outside of times of immediate crisis, might better encourage entities to share information during and in the aftermath of a cyber incident than a compliance-focused approach.

Measure 4: Cyber Incident Review Board

auDA supports the policy objective of establishing a mechanism for independent review of the root causes of cyber incidents, assessing the effectiveness of post-incident response, and disseminating recommendations and lessons learned. It is important that such reviews are seen as fact finding, knowledge sharing root cause processes rather than fault finding exercises.

We believe there could be value in further considering a cyber incident review mechanism comprising both government officials and respected industry experts (peers) to facilitate this. Any new mechanism should ensure both cyber security expertise and impartial industry expertise from the relevant sector.

As mentioned above, while sharing information across industry and government can assist entities to strengthen their defences, the Consultation Paper notes existing industry reluctance to share information with government may be due to the shift to a compliance-based approach. Legislating a new body with mandatory powers is unlikely to reduce this reluctance and does not appear necessary at this stage. We note there are already mechanisms through which an entity could be compelled to provide information (such as regulator investigations or parliamentary inquiries). We consider a model similar to the United States Cyber Safety Review Board, with its emphasis on fact-finding and making recommendations on lessons learned, could be considered in the first instance.

Decisions on whether to launch a review should be tied to the impact of a particular incident, and whether a review is likely to lead to better understanding or offer any new lessons. Issues to consider might include the number of people affected, the duration of any service outages, the consequences of any service outages, and the significance of any flow on effects to the community arising from an incident (such as disclosure of personal information and sensitive information).

PART TWO: Amendments to the Security of Critical Infrastructure Act 2018

Measure 5: Protecting critical infrastructure - data storage systems and business critical data

auDA notes the proposed amendments have the potential to interact with the Privacy Act, which is being reviewed. We recommend close coordination across government to avoid any conflicting or duplicative obligations on industry.

We consider auDA's "business critical data" to be the .au registry database, which is already publicly declared under the SOCI Act as a critical asset as part of the domain name system.

Our other data storage systems are not directly connected to the critical infrastructure.

auDA considers supply chain risks, including data storage, as part of our existing risk management including our commitment to the Information Security Management Standard ISO 27001:2022. We do not anticipate that the proposed amendments will significantly impact on our operations or our ability to use data for business purposes.

Measure 6: Consequence management powers

We recognise there is a community expectation that governments are able to deal with the consequences of any major cyber incident, including where there may be flow on non-cyber effects to an entity's customers or members of the public.

While we acknowledge the policy intent of the proposed amendment, we consider the government assistance measures in Part 3A are already significant powers and we are cautious about the potential expansion of these.

It is not clear what would be included within the scope of "consequence management". While we understand it is intended to be a last resort power, it is potentially a very broad power. We consider clarification of the definition is required.

We do not consider the proposed safeguards provide appropriate oversight. While we welcome the requirement for the Minister for Home Affairs to consult with an affected entity, we seek further clarification of how the legitimate interests of an entity subject to the direction would be considered, particularly where the entity was not involved in the initial cyber incident.

We consider further consultation on this measure is required.

Measure 7: Protected information provisions

auDA considers it would be helpful for entities to better understand when they can disclose protected information about their critical infrastructure assets for the purposes of operation or managing risks related to them. We support clarification of the operation of the protected information provisions in the SOCI Act.

Measure 8: Review and remedy powers

The introduction of a written directions power to allow a regulator to direct a critical infrastructure entity to remedy a deficient risk management program where that entity is unwilling to comply with the regulator's recommendations seems a reasonable measure. We consider the directions power should be clearly defined and only be used in cases of serious deficiencies such as addressing material risk to national security or socioeconomic stability.

auDA's purpose is to operate the .au ccTLD for the benefit of all Australians. We believe our existing risk management plan and processes are already at a high maturity level and we do not consider the proposed power would have a significant impact on auDA's approach to preventative risk.

Summary

auDA supports the policy objectives set out in the Consultation Paper, and we appreciate the willingness of the department to engage with industry on developing these new measures. We note that some of the proposed measures have the potential to overlap with other legislation, and we encourage close coordination across government to reduce the risk of conflicting or duplicative obligations on industry.

We are supportive of efforts to increase sharing information between industry stakeholders and with government to better understand the threat environment and strengthen defences against known threats.

The Consultation Paper acknowledges that industry stakeholders are already reluctant to share information with government, and that the shift to a compliance-based approach may be contributing to this reluctance. With this in mind, we suggest a renewed focus on building trust through two-way information exchange outside of times of crisis may increase voluntary cooperation and result in more useful information than further compliance measures.

In relation to new measures, such as establishing a ransomware reporting obligation and/or a cyber incident review mechanism, we believe the focus should be on increasing community safety through better knowledge of threats and sharing of lessons learnt rather than on compliance or penalising victims of attacks.

We believe the consequence management powers are unclear and potentially very broad. The definition of what is in scope of consequence management should be clearly set out along with the avenues for appeal.

Overall, we believe further clarity on the relationship between the proposed measures is required, particularly around how information provided by industry will be used, shared and protected.

auDA would welcome further engagement and consultation with the department on the proposed reforms and implementation of the *Australian Cyber Security Strategy 2023-2030*.

If you would like to discuss our submission, please contact auDA's Internet Governance and Policy Director, Jordan Carter on jordan.carter@auda.org.au.

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

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

February 2024