Submission to the Parliamentary Joint Committee on Intelligence and Security:

Inquiry into the Cyber Security Legislative Package 2024

October 2024

.auDA

Contents

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.

As part of the communications sector, the Australian domain name system has been declared as a *critical domain name system*, under the *Security of Critical Infrastructure (SOCI) Act 2018*, and auDA has been declared as the entity that is critical to the administration of the Australian domain name system.

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.

Submission

auDA appreciates the opportunity to share our feedback on these important legislative reforms that are before the Parliamentary Joint Committee for Intelligence and Security for consideration.

We have previously made submissions to the Department of Home Affairs (the Department) on the exposure drafts of these bills and, before that, in response to the release of the Australian Cyber Security Strategy.

Our submission raises several key issues that auDA does not feel have been addressed by the Department - issues that warrant the Committee's close attention.

In making this 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* and we are pleased to offer comment on the Cyber Security Legislative Package 2024.

Cyber Security Bill 2024 and Intelligence Services Act Amendment Bill

Ransomware reporting obligations

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 should be clarified.

auDA acknowledges the rationale of limiting the scope of the proposed obligation to entities with a turnover above $3 million and agrees 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.

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 (e.g. medical clinics), as defined in the *Privacy Act 1988* (Privacy Act). A ransom or cyber extortion attack on these businesses could have significant consequences for a local community. It may be appropriate to consider extending the reporting obligation to any business that stores sensitive information, as defined in the *Privacy Act*.

Coordination of major cyber security incidents – 'limited use' obligation

In the Cyber Security Legislation Consultation Paper, the Department 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.

Public commentary from regulators following the announcement of these reforms will not alleviate concern and hesitation. From auDA's observation, the limited use obligations currently proposed are 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 noted 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.

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 also support the Board having the powers to leverage the knowledge of industry experts who would bring unique insights to a review via the proposed Expert Panel.

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. We note there are already mechanisms through which an entity could be compelled to provide information (such as regulator investigations or parliamentary inquiries).

Decisions as to whether to launch a review should be related 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).

Security of Critical Infrastructure and Other Legislation Amendment (Enhanced Response and Prevention) Bill 2024

Managing consequences of impacts of incidents on critical infrastructure assets

We recognise there is a community expectation that governments can 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 of the *Security of Critical Infrastructure Act 2018* 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 very broad. We consider clarification of and further consultation on the definition is required.

We do not consider the current 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.

Summary

As the steward of the .au domain, a part of Australian critical infrastructure, auDA supports and appreciates the policy objectives of the legislation.

While it is our understanding that the proposed amendments will have limited additional operational impact on our assets, we remain concerned that some proposed measures may bring with them unintended consequences.

Primarily, the intended Departmental intent behind these regulatory changes is to increase information sharing. 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 that 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 legislating further obligations.

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 reliance on compliance mechanisms or penalising victims of attacks.

We believe the consequence management powers are unclear and, as currently drafted, too 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 the consultation process on these reforms would benefit from greater time to deepen the good will between industry and government in the critical area of cyber security.

The journey to a more cyber secure Australia must be a genuine partnership between government and industry and will only be achieved by taking adequate time to consult and receive input from all relevant parties.

If you would like to discuss our submission, please contact auDA's Internet Governance and Policy Director, [redacted]

.au Domain Administration Limited
www.auda.org.au

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

October 2024