August 2021

Submission to Department of Home Affairs Consultation Paper

Strengthening Australia's cyber security regulations and incentives

.auDA

Introduction

auDA

au Domain Administration Limited (auDA) is the .au Country Code Top Level Domain (ccTLD[1]) administrator and self-regulatory policy body.

We are endorsed by the Australian Government and through agreement with the global Internet Corporation for Assigned Names and Numbers (ICANN) to oversee the operation and management framework of the .au domain of the Internet.

Our purpose is to provide a safe, secure, and reliable namespace for the benefit of all Australians. Our vision is to unlock positive social and economic value for Australians through an open, free, secure and global Internet. To achieve this, we perform the following functions:

- develop and implement domain name policy through multi-stakeholder processes
- promote the principles of competition, fair trading and consumer protection
- maintain technical management of the .au domain name system (DNS)
- operate a complaint handling function and facilitate the .au Dispute Resolution Policy
- license the registry operator for the central .au domain name registry
- accredit registrars, who validate and issue domain name licences
- represent .au at international fora, such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the Asia Pacific Top Level Domain Association (APTLD).

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 industry 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.

[1] 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, and gov.au.

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 and secure 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 all Australians. We recognise the impact that legislative burden can have on innovation in the technology sector and encourage the use of incentives and self-regulation where possible and a consultative approach to regulation where that is needed.

Given auDA's role in securely managing the .au, a part of Australia's critical infrastructure, and our advocacy principles to support an open, free and secure Internet, we welcome the opportunity to provide input to the Department of Home Affairs (the Department)'s consultation paper *Strengthening Australia's cyber security regulations and incentives*.

We note we have previously provided, and continue to provide, input to the Department's consultation on the *Security of Critical Infrastructure Act 2018*[2]. Our submission to that consultation speaks to our role in uplifting Australia's cyber security and the importance of cyber security more broadly. Should the Department seek more detail on auDA's submission, we would be pleased to provide it.

We look forward to continuing to engage with the Department as it progresses this important work in strengthening Australia's cyber security and offer the below comments in response to the current consultation paper.

Submission

As steward of the .au domain, a critical part of the digital economy, auDA's role is to ensure it remains stable, reliable and secure. Accordingly, cyber security is an

[2] https://www.homeaffairs.gov.au/reports-and-pubs/files/critical-infrastructure-consultation-submissions/EDS057-CISoNS-auDA.PDF; and https://www.homeaffairs.gov.au/reports-and-pubs/files/critical-infrastructure-consultation-submissions/Submission-030-auDA.PDF

enormous focus for the organisation both in our day-today operations, managing the DNS and in our research and advocacy. To this end, we offer the following observations.

Governance

Between July 1, 2019 and June 30, 2020, the ACSC responded to 2,266 cybersecurity incidents and received 59,806 cybercrime reports[3]. Throughout the pandemic, there has been an increased incidence in cyber crime across Australia[4] . Accordingly, it is more apparent than ever that the boards of Australian companies should focus their attention on cyber risk, just as they do on other business risks, such as workplace health and safety.

Companies should consider the value of including at least one non-executive director with strong IT governance and cyber security skills on their Board. Companies should also consider engaging independent cyber security auditors to review a company's cyber security controls.

auDA engages an independent party to undertake annual audits of its own security and the security of our accredited registrars. In instances where issues are identified, auDA takes immediate action to rectify these and ensure the continued security of the .au domain. Our experience is that independent auditing of auDA's, our registry's and registrars' cyber security approach, policies and practice is useful and assists in enhancing the security of the .au name space.

While recognising the inherent importance of governance standards related to cyber security, auDA considers that any standards should be voluntary. This will allow businesses to consider the standards that are appropriate to their operations, engage expertise relevant to their needs and manage costs accordingly.

Small business support

Given the rise in online engagement with customers, clients and suppliers, auDA considers there is likely to be significant benefit to small businesses cross Australia from a voluntary cyber security health check program.

Such a program would have the clear benefit helping to educate and support small businesses to upgrade and continually improve their cyber security, auDA also considers there may be commercial benefits for small businesses who partake in the

[3] https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf

[4] https://www.cyber.gov.au/acsc/view-all-content/advisories/threat-update-covid-19-malicious-cyber-activity-20-april-2020

program, for example, we have seen that smaller auDA accredited registrars who implemented an international standard for the management of information security (ISO 27001) have successfully leveraged this to acquire new customers.

Given the cost of cyber security incidents to the Australian economy is estimated at $29 billion per annum[5], and that business is increasingly conducted in an online environment, it is vital that businesses recognise and work to mitigate cyber risks.

The first step in this task is education and building a cyber-aware culture. auDA notes that a broad range of cyber security information and educational material is freely available to Australians and Australian businesses, including from the Australian Cyber Security Centre (ACSC), the Australian Small Business and Family Enterprise Ombudsman, the Council of Small Business Organisations Australia, Business Victoria and the Australian Institute of Company Directors. Paid courses and materials are also, of course, available.

As a basic safety measure, businesses should consider regular cyber awareness training for all staff and board directors. auDA has implemented compulsory monthly cyber awareness training for all staff and directors. This training instils a cyber-aware culture and ensures all staff can readily identify and guard against common security issues such as phishing. This training encourages ongoing vigilance against cyber threats.

auDA believes it is important that individuals and businesses remain as vigilant about cyber threats as they would to threats to their business such as physical theft. It is important therefore to make your technological defences as robust as your physical business security to deter cyber criminals and guard against attacks.

auDA conducts regular cyber security exercises to test its cyber defences and ensure they are as robust as they can be. Cyber security is not a set and forget exercise. Like physical security, it must be maintained, regularly checked and updated as technology changes.

Another consideration in the design of any cyber security health check program is ease of use and available support. In our view, information should be easily understood by a wide audience and support services that a small business could use to rectify any issues should also be identified or made available to users as part of the program to encourage small businesses to take action.

---

[5] https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/australia%E2%80%99s-cyber-security-strategy-2020

A further consideration in any program is setting a regular cadence for health checks. In auDA's experience, cyber security cannot be set and forget exercise, as security standards can change and vigilance can lapse. Security health checks must be undertaken at least annually in order to ensure continuous focus on and adherence to security standards.

Using readily available online tools to assess security may also be useful in uplifting small business cyber security. For example, the Australian Strategic Policy Institute (ASPI), with auDA's support, is working to deliver an online security assessment tool called auCheck. This tool will enable consumers to:

- check the security of their website or email service
- receive advice on steps to be taken to address security concerns.

auCheck is scheduled to be available, free of charge, later in 2021 and could readily form a part of any voluntary cyber security health check program.

Regulatory framework

auDA notes that cybersecurity in Australia is governed by range of legislation including the *Privacy Act 1988*, the *Telecommunications Act 1997*, the *Security of Critical Infrastructure Act 2018* and the *Crimes Act 1914*.

As responsibility for administration, regulation and enforcement of cyber security is distributed across government and through a range of legislative instruments, auDA notes that both inter-departmental liaison and industry consultation prior to the introduction of new legislation is critical. Such consultation will:

- ensure duplication and regulatory red tape does not proliferate
- ensure innovation in this critical sector is not inadvertently stifled
- enable the technology sector to continue to contribute to contribute $207 billion per year by 2030 to the Australian economy[6]
- enable the technology sector to continue to employ 580,000 Australians[7]
- enable Australia to become a world-leading digital economy and society by 2030, as set out in the Australian government's Digital Economy Strategy 2030[8].

Conclusion

In conclusion, auDA is an advocate for strengthening cyber security in Australia to support and enhance its digital economy. auDA notes, however, that there exists

[6] https://digi.org.au/wp-content/uploads/2019/09/Australias-Digital-Opportunity.pdf
[7] https://digi.org.au/wp-content/uploads/2019/09/Australias-Digital-Opportunity.pdf
[8] https://digitaleconomy.pmc.gov.au/sites/default/files/2021-07/digital-economy-strategy.pdf

significant body of material and support available for businesses and individuals to enable them to adopt greater cyber security practices.

auDA considers there may be room for incentives to encourage improved cyber security practices, however, cautions that additional regulatory burden, if any, should only be considered after extensive industry and community consultation.

Should the Department of Home Affairs or government wish to consult further on incentives or other mechanisms to improve Australia's cyber-security, auDA would welcome the opportunity to provide input. If you would like to discuss our submission, please contact auDA's Special Adviser Policy, Annaliese Williams, on [redacted]

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

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