Submission to Australia's 2020 Cyber Security Strategy

November 2019

.au DOMAIN ADMINISTRATION LTD

www.auda.org.au

PO Box 18315
Melbourne VIC 3001

info@auda.org.au

Contents

Introduction

What 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, conf.au, vic.au, nsw.au, qld.au, sa.au, tas.au, wa.au, nt.au, act.au, edu.au, gov.au, csiro.au, and oz.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.

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; and,
- manage and maintain a secure and stable Domain Name System.

auDA's stakeholders

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.

auDA belongs to a global community of organisations and plays an active role in representing .au at international fora, such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the Asia Pacific Top Level Domain Association (APTLD).

Background

auDA's submission is in response to the following call from the Commonwealth Government through the Minister for Home Affairs, the Hon Peter Dutton MP.

> "**Australia's 2020 Cyber Security Strategy - A call for views**
>
> 
>
>
> *The Australian Government is developing our nation's next Cyber Security Strategy as part of its commitment to protecting Australians from cyber threats.*
>
> *The new strategy will be a successor to Australia's landmark 2016 Cyber Security Strategy, which set out the Government's 4 year plan to advance and protect our interests online backed by a $230 million investment.*
>
> *The new strategy will build on this investment to position Australia to meet the rapidly evolving cyber threat environment.*
>
> *Consultation is now underway across the country to shape the new strategy's development. We are asking for your views on the steps we can take to improve the cyber security of Australian citizens, community groups and businesses.*
>
> *We have released Australia's 2020 Cyber Security Strategy - discussion paper (2MB PDF) to start the conversation. You can contribute your views by submitting a response to the questions it asks or attending an in-person event. You can also join the conversation on Twitter AuCyberStrategy.*
>
> *Why we need a new strategy*
>
> *Since the release of the 2016 Cyber Security Strategy, the cyber threat landscape has shifted and evolved dramatically.*
>
> *The magnitude of the threats faced by Australian businesses and families has increased. They will become more acute as our society and economy become increasingly connected. As the threat evolves, so too must our response."*

https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/cyber-security-strategy-2020

https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-strategy-2020-discussion-paper.pdf

Submission

Some of the first questions asked in the paper revolve around the types of cyber threats Government should focus on and the "*.. most appropriate role for Governments, industry and the community in keeping Australia cyber-secure…*".

auDA's response to this is simple.

auDA values a free and open Internet. This is vital to promote the free exchange of ideas unrestricted by the censorship or whims of Governments.

This general principle needs to be set aside where community harm outweighs the values of an Internet unhampered by censorship.

Terrorist/violent extremist content online

We have seen, for instance, the horrors of online streaming activity with the Christchurch terrorist attack in March 2019 which led to the *Christchurch Call* adopted in May 2019 in Paris.

Outlined here is part of what appears on the dedicated Christchurch Call website –

> ***"The Christchurch Call is a commitment by Governments and tech companies to eliminate terrorist and violent extremist content online. It rests on the conviction that a free, open and secure internet offers extraordinary benefits to society. Respect for freedom of expression is fundamental. However, no one has the right to create and share terrorist and violent extremist content online[1]".***

New Zealand and France are the founders of the Christchurch Call with Australia being one of the founding supporters.

Online service providers have also committed.

What this illustrates is that international civil society - and from auDA's perspective specifically where it relates to Internet governance - is prepared to accept restrictions where it is justified by the extreme circumstances.

auDA strongly supports this approach.

[1] https://www.christchurchcall.com/index.html

Questions 4 and 5

4. What role should Government play in addressing the most serious threats to institutions and businesses located in Australia?

5. How can Government maintain trust from the Australian community when using its cyber security capabilities?

auDA Response

The Government needs to provide an appropriate level of resourcing to enforcement bodies (as defined in the Privacy Act) to enforce the existing laws that Australia has to protect consumers, institutions and business located in Australia.

auDA has held discussions with Government law enforcement and security agencies regarding cybersecurity threats that may impact large numbers of people in Australia.

Meetings and follow-up discussions have been held with the Australian Signals Directorate, Australian Cyber Security Centre, Australian Federal Police along with Government Departments – Department of Home Affairs, Attorney-General's Department and the Department of Communications and the Arts.

auDA has developed an approach where Australian Government enforcement bodies or intelligence agencies can make a request to auDA to suspend or cancel a domain name, if it is in the public interest. auDA has defined public interest as a concern common to the public at large or a significant portion of the public, which may or may not involve the personal or proprietary rights of individual people. When auDA receives a request, the enforcement agency must identify how suspending or cancelling a domain name meets one or more of the following public interest objectives:

- proper administration of government
- the judicial system
- public health and safety
- national security
- the prevention and detection of crime and fraud
- consumer protection
- the economic wellbeing of Australia
- complying with Australia's obligations under international law
- the integrity, stability or security of the Domain Name System
- auDA values continuing collaboration with the Government and its agencies to protect Australians.

Questions 6 to 13

6. What customer protections should apply to the security of cyber goods and services?

7. What role can Government and industry play in supporting the cyber security of consumers?

8. How can Government and industry sensible increase the security, quality and effectiveness of cyber security and digital offerings?

9. Are there functions the Government currently perform that could be safely devolved to the private sector? What would the effect(s) be?

10. Is the regulatory environment for cyber security appropriate? Why or why not?

11. What specific market incentives or regulatory changes should Government consider?

12. What needs to be done so that cyber security is "built in" to digital goods and services?

13. How could we approach instilling better trust in ICT supply chains?

auDA Response

auDA believes that service providers in the IT industry should strive to improve the security available in their offerings for consumers.

Each industry sector should identify appropriate minimum security controls and standards that protect consumers, and encourage all providers of services in that industry to adhere to those standards. For example, the car industry and electrical appliance industry has steadily improved the safety standards of their products, and consumers trust that in purchasing these products that they are protected. A similar approach can be applied with respect to the cybersecurity safety aspect of products.

auDA has set minimum security standards for registrars that provide domain name services for consumers, institutions and businesses. auDA also requires that registrars undergo regular independent security audits to confirm that they are complying with the minimum-security standards. auDA is in the process of releasing new standards that incorporate industry best practice such as identified in the ASD Essential Eight and ISO 27001 Information Security Management System. For example, requiring that registrars patch their software regularly and provide their customers with multi-factor authentication. auDA will require that registrars are certified against the international security standard ISO 27001.

auDA encourages the use of third parties to conduct regular vulnerability scans and red-team penetration testing for systems that hold large quantities of consumers' personal information.

Just as most organisations require an independent audit of financial results and financial controls, organisations should also require an independent audit of their security systems.

The Government can influence the supply chain by requiring that vendors that supply services to Government meet minimum security standards, and also require those vendors to regularly undergo independent security audits.

The Government can also continue to invest in consumer education so that consumers can be informed buyers of goods and services, and request that vendors have appropriate security features.

With respect to services such as website design and web hosting, most consumers, institutions and businesses don't have the skills to determine whether the service provider is taking security seriously. auDA has sponsored a project with the Australian Strategic Policy Institute (ASPI) to build a free website testing service.

This will be a public facing security web-based tool.

For Australia's Internet users, the tool will be able to check the security of websites set against a set of requirements such as HTTPS and DNSSEC.

The program is designed to promote public trust and confidence in Australia's online services along with the adoption of modern Internet standards that improve security.

The tactical objectives are to advocate (e.g. public awareness), to educate (e.g. interpreting results) and to validate (e.g. the test tool and test report).

The tool will also be scalable to include, potentially, assessment of whether Content Management Systems in use on websites are running the latest versions that incorporate up-to-date security patches.

The Government has been briefed on the program, for instance through the Digital Transformation Agency, the eSafety Commissioner and the Department of Communications and the Arts. This followed a wider consultation phase, including through the Joint Cyber Security Centres.

We are now in year two of development. auDA is making a significant investment in the initiative to keep Australians cyber safe.

Beta acceptance testing will be carried out until the end of 2019 – with the confirmed involvement and support of Cloudflare, one of the world's leaders in Internet security - with a possible public launch in February 2020.

This which will be accompanied by an education and awareness campaign.

Key roles for Government include:

- Ensuring the Government itself uses industry best practices to protect information about Australian consumers, including publishing the high-level results of independent security audits of their systems.
- Ensuring the Government demands minimum cybersecurity standards in the products it purchases from vendors and requires that vendors undertake regular independent security audits of their systems.
- Investing in consumer education to ensure that consumers demand appropriate cyber-security protections for the goods and services they purchase (for example most consumers will request that sunglasses have appropriate UV protections based on previous consumer awareness campaigns).

Question 14

14. How can Australian governments and private entities build a market of high-quality cyber security professionals in Australia?

auDA Response

auDA is investing in its IT staff through sending them to local and international cyber security conferences, and investing in further cyber security training. All staff undergo cyber-awareness training with monthly online tutorials and regular tests of cyber security awareness (e.g. through sending examples of phishing emails).

Governments can help build a market for high quality cyber security professionals by funding training for their existing IT staff to improve their knowledge of cyber security, and providing higher wages to those that have successfully completed cyber security training.

Questions 16 to 21

16. How can high-volume, low-sophistication malicious activity targeting Australia be reduced?

17. What changes can Government make to create a hostile environment for malicious cyber actors?

18. How can governments and private entities better proactively identify and remediate cyber risks on essential private networks?

19. What private networks should be considered critical systems that need stronger cyber defences?

20. What funding models should Government explore for any additional protections provided to the community?

21. What constraints to information sharing between Government and industry on cyber threats and vulnerabilities?

auDA Response

auDA actively monitors spikes in DNS queries for domain names in .au and, if necessary, engages with the Australian Cyber Security Centre regarding mitigation and future action.

Better information sharing of unusual traffic spikes, may help identify when a potential high-volume attack is being planned.

As noted earlier, Government can implement the controls recommended by ASD and the Australian Government's Information Security Manual for all Government departments to set an example for best practice. Governments can also require that suppliers of products and services to Government also meet these standards.

auDA recommends that Government and the private sector engage external companies to test for vulnerabilities, and for critical systems auDA recommends the use of external red-team penetration testing services. This ensures that Government and the private sector are proactively looking for vulnerabilities in their systems.

The .au domain name system should be considered an important system, and that is why auDA is putting in place additional security controls to meet international best practice, and using external services to validate that the controls have been configured correctly. auDA approach is to constantly test and improve its security.

One of the constraints to information sharing is ensuring that the privacy and personal information of individuals is not compromised. Where possible organisations should remove any personally identifiable data before sharing with other organisations.

Questions 22 to 25

22. To what extent to you agree that lack of cyber awareness drives poor consumer choices and/or market offerings

23. How can an increased consumer focus on cyber security benefit Australian businesses who create cyber security products?

24 What are examples of best practice behaviour change campaigns or measures? How did they achieve scale and how were they evaluated?

25. Would you like to see cyber security features prioritised in products and services?

auDA Response

auDA agrees that a lack of cyber awareness drives poor consumer choices.

For example, the .au ccTLD requires validation of the domain name licence holder before issuing a domain name licence. The holders of a .au domain name licence need to have an Australian presence, which means they can be held accountable under Australian law for the use of that name. The holder of a com.au domain name licence is typically a registered company with an ACN number, or a sole trader with an ABN number. auDA displays the name and identifier (e.g. ACN or ABN) of the domain name holder in the public WHOIS directory https://whois.auda.org.au/. This means consumers can identify the company or person that has registered a domain name, and additional information is available through other Government databases such as the ASIC company database and the Australian Business Number database. auDA also has a complaints system to cancel domain name licences, where the domain name licence holder is not, or is no longer, eligible to hold a domain name licence within the .au ccTLD.

In contrast, other domain name spaces like .com require no connection with Australia and have minimal validation of the domain name holder. Increasingly the WHOIS information about the .com name is not publicly available.

auDA believes that consumers have much better protection under Australian law if they interact with a natural person or business that is using a domain name within the .au ccTLD.

To improve access to domain names within the .au ccTLD, auDA is creating the option for natural persons and micro-businesses, that don't have an ABN or ACN number to be eligible to register in com.au, to register directly at the second level of .au (e.g. *forexample.au*).

auDA recommends that the Government encourage Australian consumers, institutions and businesses to register their domain name within the .au ccTLD. auDA also recommends that the Government assist in raising consumer awareness that they are better protected under Australian law if they interact with a natural person or organisation using a domain name within the .au ccTLD (i.e. .au, com.au, net.au, org.au, asn.au, id.au, conf.au, vic.au, nsw.au, qld.au, sa.au, tas.au, wa.au, nt.au, act.au, edu.au, gov.au, csiro.au, and oz.au), compared to other domain namespaces.

A focus on the benefits of dealing with natural persons, institutions and businesses that can be held accountable under Australian law will also have the benefit of ensuring that more dollars are spent within the Australian digital economy. See the ACIL Allen Consulting report on Direct Registration in Australia: https://www.auda.org.au/assets/Policies/panels-and-committees/2017PRP/auDA-PRP-Direct-Registration-in-Australia-Cost-Benefit-Analysis-ACIL-ALLEN.pdf

Cyber awareness training needs to be part of education within schools, universities and within corporate training programs. For example, auDA requires all staff to participate in ongoing cyber awareness training, with monthly tutorials and participate in regular simulations of cyber attacks. An increased awareness of cyber security issues will likely lead to consumers demanding more cyber security features from their suppliers of products and services.

Question 26

26. Is there anything else that Government should consider in developing Australia's 2020 Cyber Security Strategy?

auDA Response

auDA has approved the introduction of direct registration at the second level (e.g. *myname.au*) and is currently undertaking a round of consultation regarding the fine details of the new Licensing Rules.

This will, by definition, allow shorter and more memorable names, but will also encourage Australian Internet users to remain within the *.au* ccTLD rather than favouring registrations through, for instance *.com* or other Top Level Domains (TLDs).

Better choice and take-up of .au has a flow-on security and consumer benefit with registrants having the protection of local robust Australian oversight.

Summary

auDA remains supportive of the Government's priority to keep Australians cyber safe and promote stability and security in our online activities.