.au Domain Administration

Supplementary Submission to Department of Home Affairs *Protecting Critical Infrastructure and Systems of National Significance*

21 September 2020

.au DOMAIN ADMINISTRATION LTD

www.auda.org.au

PO Box 18315
Melbourne VIC 3001

info@auda.org.au

Contents

Executive Summary

- .au Domain Administration Limited (auDA) takes security extremely seriously and benchmarks against international best practice
- auDA's DNS systems are globally distributed for scale and reliability, and to handle the high proportion of international DNS queries for .au domains
- auDA accredited registrars are globally distributed
- The internet resources (including web and email servers) referenced by domain names in the .au ccTLD are globally distributed
- auDA has international obligations to manage and preserve the universality, interoperability and accessibility of the Public Core of the Internet
- The Australian Government's international position is that no government should regulate the Internet, and that a multi-stakeholder model of internet governance is the most effective mechanism to develop public policy positions across the full spectrum of cyber affairs
- auDA believes that the existing Australian Government terms of Endorsement and the reserve powers in the Telecommunications Act already provide sufficient mechanisms for the Government to provide oversight of auDA

Introduction

1. .au Domain Administration Limited (auDA) welcomes the opportunity to make a supplementary submission to the Department of Home Affairs *Protecting Critical Infrastructure and Systems of National Significance Consultation Paper.* This submission should be read in conjunction with the short submission made by auDA on 16 September 2020.

2. While auDA welcomes the Australian Government's policy commitment to an all-hazards approach to protecting critical infrastructure, the proposed critical infrastructure (CI) reforms are designed to enhance the capability of the government and critical infrastructure operators and owners to 'manage the national security risks of espionage, sabotage and coercion arising from foreign involvement in Australia's critical infrastructure.'[1] In this context, auDA believes that the application of these CI reforms to the .au ccTLD raises significant public policy issues relating to the securitization of the Internet.

3. auDA is willing to work with the Department of Home Affairs ('the Department') to identify the potential consequences of DNS infrastructure disruption and to establish appropriate risk mitigation strategies. auDA is happy to facilitate a workshop with the Department and auDA's accredited Registrars[2] and DNS infrastructure providers to work through the potential impacts of the CI reforms on the .au Domain Name System (DNS).

4. auDA has provided an overview of the Domain Name System and .au country code Top Level Domain (ccTLD) at Attachment A.

Background

.au Domain Administration Limited

5. auDA is the administrator of and the Australian self-regulatory policy body for the .au country code Top Level Domain (ccTLD). auDA performs this role pursuant to the Australian Government Terms of Endorsement[3] and the Internet Corporation for Assigned Names and Numbers (ICANN) Sponsorship Agreement.[4] In performing these functions, auDA has:

    (a) international obligations to manage and preserve the universality, interoperability and accessibility of the Public Core of the Internet; and

    (b) domestic obligations to manage the .au ccTLD in the public interest, subject to Australian Government requirements.

6. The division of authority between the Australian Government and ICANN is:

[1] Explanatory Memorandum, Security of Critical Infrastructure Bill 2017, 1 [1].
[2] auDA accredits Registrars to provide Registrar Services, including the registration of domain names.
[3] Australian Government, Department of Communications and the Arts, Review of the .au Domain Administration: Terms of Endorsement (issued 16 April 2018) <https://www.communications.gov.au/documents/review-au-domain-administration-terms-endorsement>
[4] Internet Corporation for Assigned Names and Numbers, ccTLD Sponsorship Agreement (.au) (25 October 2001) < https://www.icann.org/resources/unthemed-pages/sponsorship-agmt-2001-10-25-en>

(a) the Australian Government has sovereign rights over the delegation and administration of the .au ccTLD[5] ; and

(b) ICANN has authority over the global technical coordination to ensure that the Internet domain name system continues to provide an effective and interoperable global naming system[6].

Terms of Endorsement

7. The Australian Government Terms of Endorsement (TOE) provide that 'responsibility for the administration of .au is ultimately derived from and is subject to, the authority of the Commonwealth. The Australian Government can delegate the responsibility for managing the .au namespace to an appropriate entity or organization.'[7] The Australian Government endorsement of auDA as the .au administrator is contingent on auDA administering the .au in the public interest and performing the following core functions, among others:

- ensure stable, secure and reliable operation of the .au domain space
- respond quickly to matters that compromise DNS security[8]

8. In performing these functions, auDA is required to:

- engage with key international security fora to ensure it is aware of international security developments and best practice
- develop, maintain and, to the greatest extent possible, publish an enterprise security strategy which is informed by domestic and international best practice
- work with the Department of Communications and the Arts to facilitate partnerships between auDA and relevant cyber security agencies[9]

9. The Australian Government through the Department of Infrastructure, Transport, Regional Development and Communications (DITRDC) retains supervisory oversight of auDA, including:

- receiving quarterly reports on performance and work priorities
- right to independently review auDA's reporting and reporting processes at any time

[5] Australian Government Terms of Endorsement (dated 31/12/2000); Clause 1.10 of the ccTLD Sponsorship Agreement (.au) (https://www.icann.org/resources/unthemed-pages/sponsorship-agmt-2001-10-25-en); Paragraph 4.1.1 of the Government Advisory Committee, Internet Corporation for Assigned Names and Numbers, Principles and Guidelines for the Delegation and Administration of Country Code Top Level Domains (5 April 2005); https://gac.icann.org/principles-and-guidelines/public/principles-cctlds.pdf

[6] Internet Assigned Numbers Authority, IANA Report on request for Redelegation of the .au Top Level Domain (31 August 2001) https://www.iana.org/reports/2001/au-report-31aug01.html; Clause 1.10 of the ccTLD Sponsorship Agreement (.au) (https://www.icann.org/resources/unthemed-pages/sponsorship-agmt-2001-10-25-en

[7] Australian Government, Department of Communications and the Arts, Review of the .au Domain Administration: Terms of Endorsement (issued 16 April 2018) 1.

[8] Ibid

[9] Ibid 3

- a senior officer from the DITRDC is included in all relevant auDA governance processes, including, but not limited to, non-voting observer status at board meetings for all decisions.[10]

10. The Australian Government also has reserve powers under sections 474-477 of the *Telecommunications Act 1997* (Cth) and sections 11 and 17 of the *Australian Communications and Media Authority Act 2005* (Cth) to provide for intervention in the event that auDA is unable to manage electronic addressing in an effective manner.

ICANN Sponsorship Agreement

11. The ICANN Sponsorship Agreement sets out the technical responsibilities and obligations of ICANN and auDA in managing the .au ccTLD zone to ensure the "technical stability and operation of the DNS and Internet in the interest of the global internet community."[11] The ICANN Sponsorship Agreement requires auDA to:

    (a) to ensure the stable and secure operation and maintenance of the authoritative primary and secondary nameservers[12]

    (b) provide ICANN with access to zone files and registration data for the .au ccTLD for the purpose of verifying and ensuring the operational stability of the .au ccTLD[13]

    (c) ensure the safety and integrity of the registry database, including the establishment of an escrow or mirror site for the registry data[14]

    (d) requirement to keep the .au ccTLD technical and administrative contact details up to date

    (e) conformity to ICANN policies relating to the interoperability of the .au ccTLD with other parts of the DNS and Internet, operational capabilities and performance of auDA, and the obtaining and maintenance of, and public access to, accurate and up to date contact information for registrants[15]

    (f) comply with the technical specifications set out in Attachment F, including operating the database with accuracy, robustness and resilience.[16]

12. ICANN can terminate the Sponsorship Agreement where, among other matters:

    (a) auDA acts or continues acting in a manner that ICANN reasonably determined endangers the operational stability of the DNS or the Internet[17]

---

[10] Ibid
[11] Internet Corporation for Assigned Names and Numbers, ccTLD Sponsorship Agreement (.au) (25 October 2001) [1.10]
[12] Ibid[4.1]
[13] Ibid[4.2]
[14] Ibid[4.3]
[15] Ibid[4.5]
[16] Internet Corporation for Assigned Names and Numbers, ccTLD Sponsorship Agreement (.au) (25 October 2001), Attachment F <https://www.icann.org/resources/unthemed-pages/sponsorship-agmt-attf-2001-10-25-en>
[17] Internet Corporation for Assigned Names and Numbers, ccTLD Sponsorship Agreement (.au) (25 October 2001)[6.2.3]

(b) the Australian Government notifies ICANN that it has withdrawn its endorsement of auDA as an appropriate person to manage the .au ccTLD.[18]

13. On termination of the agreement, auDA has a surviving obligation to cooperate with ICANN to transfer the operation of the .au ccTLD to another party endorsed by the Australian Government.[19]

Corporate Constitution

14. auDA is required to operate within its Constitution under the Australian Government TOE. [20] The objects of the Constitution set out the technical and regulatory functions of auDA as the .au ccTLD administrator.

15. auDA technical functions are:

(a) maintain and promote the operational stability and utility of the .au ccTLD and more generally, the internet's unique identifier system and to enhance the benefits of the internet to the wider community,[21] and

(b) to manage the operation of critical technical functions including the primary and secondary nameservers, zone files for the second level domains (2LDs) and a searchable database (https://whois.auda.org.au/) containing information on registrations within the .au ccTLD.[22]

16. The self-regulatory policy functions, which enable auDA to make and enforce rules governing the accreditation of registrars and registry operators,[23] and the rules governing the registration of domain names in the second level domains (2LD)[24] are an important tool in improving the overall security posture of the .au DNS. For example, auDA requires all auDA accredited Registrars to comply with the Information Security Standard for Accredited Registrars. The registration rules operate as a barrier to entry into the .au domain for malicious actors or cyber criminals as there is a requirement that a person has an Australian nexus and that registrars verify registrant information prior to submitting an application for a domain name to the registry.[25]

Public Core of the Internet

17. The Domain Name System (DNS) is part of the Public Core of the Internet, which comprises the following layers:

(a) logical layer – applications, data and protocols that allow exchange of data, such TCP/IP, DNS and routing protocols

---

[18] Ibid[6.2.4]
[19] Ibid [6.3]
[20] Australian Government, Department of Communications and the Arts, Review of the .au Domain Administration (April 2018)
[21] Constitution of .au Domain Administration Limited, cl 1.2(b)
[22] Ibid cl 1.2(e)
[23] Ibid, cl 1.2d(iii)
[24] Ibid, cl 1.2(iv)
[25] 2012-04 Domain Name Eligibility and Allocation Policy Rules for the Open 2LDs, Schedule 1; 2012-05 Guidelines on the Interpretation of Policy Rules for Open 2LDs, para 6.

(b) Physical layer compromising the physical network components (hardware and other infrastructure such as telecommunication cables, Internet routers, DNS nameservers, and computers)

(c) Organizational layer such as internet exchanges, Computer Emergency Response Teams (CERTs), Registrars, Top Level Domain (TLD) Registries, TLD administrators and policy settings.

18. The Public Core of Internet only works properly if its underlying values of universality, interoperability and accessibility are guaranteed. In 2018, the 'five country' Ministers reaffirmed their vision of a "free, open, safe and secure internet."[26] Canada, United States of America, New Zealand, and Australia have not subscribed to the infrastructure in Internet governance approach adopted by other States, preferring to influence the behaviour of ccTLD administrators through non-legislative mechanisms.

Thematic Issues

Critical Infrastructure

19. auDA welcomes the Department's commitment to working with industry to identify and map assets and entities that may be critical infrastructure, including systems of national significance.[27] auDA provides these comments to assist the Department in forming a view as to whether auDA should be considered 'critical infrastructure' for the purposes of the proposed reforms and to assess the regulatory impact of these reforms on the operations of auDA as the .au ccTLD administrator.

20. DITRDC in its 2018 Review of .au Domain Administration did not go as far as identifying the .au ccTLD as critical infrastructure. DITRDC found that as auDA falls within the telecommunications sector which is a critical infrastructure sector under the Australian Government Critical Infrastructure and Resilience Strategy, it is therefore part of the critical infrastructure sector.[28] However, auDA is not subject to Part 14 of the *Telecommunications Act 1997* (Cth) (Telecommunication Sector Security Reforms).

21. auDA agrees that the .au DNS is critical infrastructure as defined in the Critical Infrastructure and Resilience Strategy,[29] as any disruption of the .au DNS may impact:

(a) the ability of critical infrastructure providers, businesses, non-government organizations and Australian governments to provide services and to communicate via the Internet; and

(b) users of these services wherever domiciled.

---

[26] Australian Government, Department of Home Affairs, Five country ministerial 2018 (accessed 18 September 2020) 1 <https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/five-country-ministerial-2018#:~:text=%20Five%20country%20ministerial%202018%20%201%20Official,spaces.%20We%2C%20the%20Homeland%20Security%2C%20Public...%20More%20>

[27] Australian Government, Department of Home Affairs, Protecting Critical Infrastructure and Systems of National Significance Consultation Paper (August 2020) 13.

[28] .Australian Government, Department of Communications and the Arts, Review of the .au Domain administration (April 2018) 14.

[29] Australian Government, Department of Home Affairs, Critical Infrastructure Resilience Strategy: Policy Statement (2015) 3.

However, the .au DNS is a network within a network. It is a system of globally distributed DNS nameservers and other infrastructure that is managed and operated by a range of parties, such as Registrars, Internet Service Providers, DNS service providers, website hosting companies, email service providers, and telecommunication providers. Its globally distributed nature raises significant issues in relation to Australian sovereignty over infrastructure outside its territorial borders.

22. auDA as the .au ccTLD administrator manages, either directly or through contracted service providers, only a small part of the overall DNS, auDA manages the:

    (a) .au top level zone

    (b) Registry database

    (c) Authoritative DNS nameservers

    (d) WHOIS registration data directory services (https://whois.auda.org.au/)

23. auDA accredits registrars to provide .au ccTLD domain name registration services, which often include DNS hosting. Registrars may also provide additional services such as webhosting and email. Registrars operate DNS infrastructure for the purposes of performing these functions. A significant proportion of auDA accredited registrars are domiciled overseas, and these registrars manage approximately two thirds of all .au ccTLD domains under management.

24. auDA has little visibility of other DNS Service Providers, such as ISPs, Webhosting companies, telecommunication providers and DNS providers (such as Cloudflare).[30] Webhosting, email service providers, and DNS providers are often domiciled overseas, such as Bluehost, Hostgator and Dreamhost.

25. The .au DNS has a large attack surface due to its globally distributed infrastructure network and .au DNS infrastructure operators. The proposed critical infrastructure reforms may create regulatory gaps due to jurisdictional issues that may make overseas auDA accredited registrars an attractive target for the purpose of espionage, sabotage and foreign interference targeting Australian critical infrastructure. The recent large-scale DNS hijacking campaigns demonstrate the national security risks of DNS compromise at the Registrar, ISP and telecommunication provider levels. Registrars and ISPs were targeted through spear phishing and other means to gain login details of DNS servers. The attackers then used these login details to change DNS server records to redirect user traffic to attacker-controlled infrastructure and to obtain valid encryption certificates for an organization's domain names, enabling man in the middle attacks.[31] The scale of these attacks against national security agencies and commercial enterprises in the Middle East was unprecedented.

[30] DNS Providers operate DNS network and software infrastructure, whereas DNS Service Providers are the businesses that you interact with to manage your online presence such as registering a domain name, accessing the Internet or hosting your website.

[31] Government of the United States of America, Department of Homeland Security, Alert (AA19-024A) DNS Hijacking Campaign (24 January 2019) https://us-cert.cisa.gov/ncas/alerts/AA19-024A; UK Government, National Cyber Security Centre, Advisory: Ongoing DNS hijacking and advice on how to mitigate (12 July 2019) https://www.ncsc.gov.uk/news/ongoing-dns-hijacking-and-mitigation-advice.

26. auDA would caution against categorizing .au DNS infrastructure as critical infrastructure and systems of national significance until the Department has time to complete a mapping exercise that (1) identifies .au DNS infrastructure and its location, (2) the operators of that infrastructure and (3) vulnerabilities within the .au DNS. auDA believes that the distributed nature of the .au DNS, and overseas infrastructure and operators may make any regulation less than optimal due to jurisdictional issues.

Current Regulatory Environment

27. The Australian Government has adopted a quasi-regulatory approach through the TOE for administering the .au ccTLD. The 2018 Review of the .au Domain Administration stated that the Australian Government "considers the TOE is an appropriate mechanism for Government in providing directions on its expectations of auDA."[32] This regulatory approach reflects the Australian Government's international position that no government should regulate the Internet, and that a multi-stakeholder model of internet governance is the most effective mechanism to develop public policy positions across the full spectrum of cyber affairs.[33] This multi-stakeholder internet governance model is reflected in the Australian Government's strong commitment to self-regulation of the .au DNS by the Australian Internet community.

28. auDA agrees that the TOE is the most appropriate mechanism through which the Australian Government should pursue its policy objectives, including ensuring the stable, secure and reliable operation of the .au domain space and responding quickly to matters that compromise DNS security.[34] The TOE have given auDA an authorizing environment in which to drive significant internal and external security reforms that aim to make the .au DNS stable, secure and resilient to a range of cyber incidents, insider threats, natural hazards and health emergencies.[35] The auDA Enterprise Security Strategy sets out all the measures that auDA takes to address security risks and robustness of its systems. [36]

29. auDA believes that transactional regulation is a more effective means of addressing security issues as it is not dependent on jurisdiction. The effectiveness of transactional regulation in addressing security risks in Registrar operated DNS infrastructure is demonstrated by the new Registrar Agreement, which will drive an uplift in the security posture of all auDA accredited Registrars. The new Registrar Agreement requires registrars to adopt and maintain an "Information Security Management System" in compliance with ISO27001 or another recognized standard as approved by auDA[37] and to implement and maintain the prescribed minimum security controls.[38] Registrars will be independently audited every 12

[32] Australian Government, Department of Communications and the Arts, Review of the .au Domain Administration (April 2018) 28.
[33] Australian Government, Department of Foreign Affairs and Australia's International Cyber Engagement Strategy (2016) https://www.dfat.gov.au/publications/international-relations/international-cyber-engagement-strategy/aices/chapters/part_5_internet_governance_and_cooperation.html
[34] Australian Government, Department of Communications and the Arts, Review of the .au Domain Administration: Terms of Endorsement (issued 16 April 2018) 1<https://www.communications.gov.au/documents/review-au-domain-administration-terms-endorsement>
[35] auDA Enterprise Security Strategy https://www.auda.org.au/assets/Uploads/auDA-enterprise-security-strategy-.pdf
[36] auDA Enterprise Security Strategy https://www.auda.org.au/assets/Uploads/auDA-enterprise-security-strategy-.pdf
[37] Registrar Agreement, cl15.1
[38] Registrar Agreement, cl 15.3

months[39] and non-compliance will result in suspension from the Registry.[40] This means that Registrars will not be able to create any new domain name registrations. The Registrar Agreement also contains Personnel security requirements in respect to access to registry data.[41]

30. auDA has also been cognizant of the impact that any disruption or degradation of the .au DNS may have on Australian businesses, government, education and non-government organizations and users of these services. To address this issue, auDA has step in rights under the new Registrar Agreement, which enables it to assist the Registrar and Registry Operator should a Force Majeure event occur and there is a potential degradation or disruption to the .au DNS.[42]

31. The Cyber Security Strategy 2020 sets out a range of measures to keep Australians safe online. auDA plays an important role in ensuring that the .au ccTLD is not used by criminals and malicious actors to target Australians. auDA will be introducing a new Licensing Scheme that will require Registrars to validate the identity and Australian presence of a person applying for a domain name in the .au ccTLD,[43] new regulatory tools such as audit and domain name suspension powers and the Public Interest Test.[44] The Public Interest Test will allow an enforcement body or intelligence agency to request the deletion, suspension or to take other action in respect to a domain name where it is in the public interest.

32. auDA supports the Government's position that "Boards of critical infrastructure entities have visibility of, and are responsible for planning and actively managing security and resilience."[45] The auDA Board has established a range of governance measures to understand and advise on security risks. The Board receives detailed monthly operational reports on the key metrics associated with the .au DNS infrastructure, and receives reports of all incidents that impact the infrastructure. The Board's Security and Risk Committee (SRC) has responsibility for oversighting and advising the Board on matters relating to security and risk, including governance and risk management, security and business continuity. With respect to security, the SRC regularly monitors the integrity of auDA's security management against applicable policies and controls, and regularly monitors and reviews security enforcing functions including, activity monitoring, end-point protection software and processes, vulnerability and/or penetration testing, and DDoS mitigation to ensure they are fit for purpose and meeting the objective of applicable security policies.

33. The Board has also appointed an external Technical Advisory Standing Committee (TASC) to receive and consider input from the Internet technical community on aspects of auDA's operations, decisions or actions and provide advice to the Board. The committee comprises people with technical expertise in IP addressing, DNS, domain name registration operations, and IT security. auDA works closely with the Australian Signals Directorate

[39] Registrar Agreement, cl 16
[40] Registrar Agreement, cl 13.1
[41] Registrar Agreement, cl 15.5
[42] Registrar Agreement, cl 23
[43] Registrar Agreement, cl 21; .au Domain Administration Rules – Registrar, para 2.4; These new rules build on the existing requirements for registrars to verify a person's eligibility to hold a domain name under paragraph 6 of the *Guidelines on the Interpretation of Policy Rules for Open 2LDs* (2012-05).
[44] .au Domain Administration Rules – Licensing, para 2.17
[45] Australian Government, Department of Home Affairs, Protecting Critical Infrastructure and Systems of National Significance Consultation Paper (August 2020)

(ASD) to both seek its advice on security matters and offer assistance in identifying Australian systems that may have been comprised by malicious software. auDA actively participates in the activities of the Melbourne Joint Cyber Security Centre (JCSC), and, until the COVID-19 lockdown, had a staff member located at the JCSC to assist collaboration and information sharing with the Government and industry.

Regulatory reform

34. auDA has been through significant reforms over the last two years as a result of the 2018 Australian Government Review of the .au Domain Administration, including substantial uplifts in its security posture and reform of its Licensing Scheme to ensure that the .au is stable, secure and trusted. The Australian Government has reaffirmed its commitment to a self-regulatory regime for the .au ccTLD.

35. auDA is unclear as to what specific failings and weaknesses in the current arrangements that the Department would be seeking to address by capturing auDA as critical infrastructure under the proposed critical infrastructure reforms ('the CI reforms'). auDA believes that any deficit that may be identified by the Department in its security arrangements can be addressed through the TOE.

36. The upcoming DITRDC review of the TOE provides an opportunity for the Department to seek to incorporate the proposed security obligations in the TOE. The benefits of this approach, include:

    (a) maintains the Australian Government position that the internet should not be regulated by governments

    (b) consistent with the self-regulatory model for administering the .au ccTLD

    (c) overcomes jurisdictional issues as auDA can use its contractual arrangements to implement the obligations across its Registrars

    (d) harnesses the role of auDA to develop and enforce policies

    (e) develops industry wide solutions to security issues

37. In the event, that this quasi-regulatory approach does not achieve the desired public policy outcomes, then the Department still has the option of:

    (a) prescribing or declaring the .au ccTLD or parts of the .au DNS as a critical infrastructure asset under section 9(1)(f) or section 51 of the *Security of Critical Infrastructure Act 2018* (Cth) ('SOCI Act') or

    (b) declare auDA as a carriage service provider for the purposes of Part 14 of the *Telecommunications Act 1997* (Cth).

38. auDA firmly believes that regulation under the SOCI Act or *Telecommunications Act 1997* (Cth) should be a last resort option due to the regulatory burden that this would place on auDA as a not for profit organization. The Australian Government recognizes that

regulation may have a disproportionate impact on not for profits compared with commercial organizations.[46]

39. auDA is a relatively small organization with a staff of 25 FTE, which are spread across its technical, corporate, and regulatory and enforcement functions. It is self-funded through the wholesale proportion of the registration fee that a person pays to a registrar when registering a domain name. This wholesale fee is shared with the Registry operator. auDA would need to employ additional staff to meet its obligations under the SOCI Act or *Telecommunications Act 1997* (Cth) to avoid having to reallocate staff from essential functions, such as compliance and enforcement, and recover the costs through increases in the wholesale licence fee.

Critical Infrastructure Reforms

Industry – Government Collaboration

40. auDA agrees that industry and government collaboration is essential to achieving an uplift in security standards across multiple critical infrastructure sectors through principles-based regulation, which provides operators with the necessary agility to respond to a rapidly evolving security and threat environment. auDA welcomes the introduction of a range of measures that will improve collaboration, such as industry-government secondment program, threat assessments and briefings. auDA has found that having an outposted compliance officer in the Melbourne Joint Cyber Security Centre has provided a range of benefits, including enabling a better understanding of the government's cyber security approach and processes, and increased collaboration and information sharing with other industry sectors.

Principles based outcomes

41. The Government's principles-based outcomes approach is welcome as it recognizes that critical infrastructure owners and operators are better placed to determine what processes and actions are required within their business to achieve the desired outcome. As a not for profit, auDA welcomes the flexibility to choose the most appropriate and cost-effective way of achieving any regulatory obligations.

42. The principle based outcomes that require an entity to (1) understand risks, (2) mitigate risks to present incidents, (3) minimize the impact of realized incidents and (4) effective governance and high level security obligations relating to physical, cyber, personnel and supply chain security appear to be reasonable, and appropriate response to an all hazard approach to critical infrastructure protection.

43. While supportive of principles-based regulation, auDA is concerned that to be an effective form of legislation that it will need to be supplemented by detailed regulations, standards, and guidelines. The Government has committed to working with industry to co-design sector specific standards that are proportionate to risk in respect of the positive security obligations. auDA welcomes this commitment and would encourage the Department to establish Implementation Working Groups across all sectors. However, there is no detail in the Consultation paper as to the regulation and rule making powers. auDA notes that the Minister has a broad rule making power under section 61 of the SOCI Act, which includes

[46] Australian Government, Department of Prime Minister and Cabinet, Office of Best Practice Regulation, Community organisations (March 2020)

"the making of rules necessary or convenient to be prescribed for carrying out or giving effect to the Act." auDA is concerned that the regulation and rule making powers may lead to regulatory creep and strongly advocates for legislative criteria that restrict the matters for which these powers can be used.

Enhanced Cyber Security Obligations

44. auDA is concerned about the lack of transparency in respect to the Enhanced Cyber Security Obligations, which appear to be a significant expansion of national security agencies' powers. auDA acknowledges that the high level description of these powers means that any comments are a 'stab in the dark' as to the operation and implication of the Enhanced Security Obligations.

Systems of National Significance

45. auDA notes that the Enhanced Cyber Security Obligations will only apply to systems of national significance. The Consultation paper does not define a system of national significance but lists two factors that will be considered (1) interdependency with other functions and (2) consequence of the compromise. Arguably, the .au DNS is a system of national significance as critical infrastructure operators, governments, education service providers, businesses and non-government organizations rely on it to provide services via the Internet and for communication. Any disruption of the .au DNS depending on the level targeted within the .au ccTLD hierarchy will have a significant impact on service providers and the broader Australian community.

46. The criteria for determining what is a system of national significance are extremely broad and subjective, given the nature of the Enhanced Cyber Security Obligations. auDA recommends that any definition contains threshold requirements and safeguards to prevent scope creep. Government should be required to consult with a critical infrastructure owner and operator before an asset can be declared a system of national significance, and any declaration should be subject to challenge by the asset owner or operator and subject to scrutiny by an appropriate oversight body.

Situational awareness

47. auDA supports the Australian Government proposal to improve owners and operators' planning and preparedness against cyberattacks. auDA supports in principle information sharing with Government for the purpose of establishing a 'near real time threat picture' but is concerned about the potential blurring of the boundary between threat intelligence and surveillance. auDA seeks further clarity on:

    (a) who in Government can issue a request for information,

    (b) the time frames for responding to a request

    (c) the time frame a request can be in force (i.e. 6 months or ongoing)

    (d) rules governing disclosure and information sharing and information retention

48. auDA is also cognizant that there are significant jurisdictional issues that may arise from collecting and using data from its global network of .au DNS nameservers. The majority of .au nameserver traffic originates from overseas, and the privacy and data implications which may arise warrant careful consideration.

Directions and Direct Action

49. The Cyber Security Strategy 2020 states that "in consultation with critical infrastructure owners and operators, Government will develop new powers proportionate to the consequences of a sophisticated and catastrophic cyberattack, accompanied by appropriate safeguards and oversight.' However, the Consultation paper only provides a high level summary of the proposed directions and direct action powers, making it difficult to grasp how these powers will work, who in Government will exercise these powers, and what, if any, accountability and transparency mechanisms will apply.

50. The directions power will be enlivened where there is an imminent cyber threat or incident that could significantly impact Australia's economy, security or sovereignty and the threat is within the capacity of the critical infrastructure operator to address. The Government can provide reasonable, proportionate and time-sensitive directions to entities to ensure action is taken to minimize its impact. Based on this description, the proposed Ministerial directions power appears to remove the thresholds and safeguards in the existing Ministerial directions powers under section 32 of the SOCI Act or section 315B(2) of the *Telecommunications Act 1997* (Cth). It is unclear why a new directions power is needed.

51. auDA strongly advocates that the proposed directions power be subject to stringent issuing criteria, including a requirement to negotiate or consult with a critical infrastructure operator in good faith. auDA believes that critical infrastructure operators are best placed to understand the nature of the threat, and its impact on their systems and customers and appropriate mitigation strategies.

52. The Consultation paper has not provided sufficient detail to understand how the direct action power would work, except that in an emergency the Government could take direct action to defend and protect the network and systems of critical infrastructure entities and systems of national significance. It is not clear if the direct actions power would allow the Government to act in anticipatory self defence.

53. auDA welcomes the Government's advice that these powers will be "accompanied by appropriate safeguards and oversight. As there is no detail as to what these safeguards and oversight mechanisms may be, auDA suggests consideration be given to:

    (a) conferring an authorisation power on the Court

    (b) right to appeal a decision relating to a request for information and directions

    (c) administrative oversight by the Inspector-General of Intelligence and Security where the authority is an intelligence agency

    (d) periodic review of the directions and direct action powers by the Parliamentary Joint Committee on Intelligence and Security.

Consultation

54. auDA believes that the Consultation paper is too abstract to really understand the obligations being proposed by Government and how they will impact on the operations of auDA as the administrator of the .au ccTLD and other DNS infrastructure providers. auDA is particularly concerned about the directions and direct actions power, and the legal immunities that may attach to the actions of government when 'it all goes wrong'.

55. auDA welcomes the Department's advice that it will be provided with an Exposure Draft of the Bill and given an opportunity to comment. However, auDA is concerned that given the legislative time-line presented at the workshops, that there will be insufficient time for genuine and considered consultation. auDA would welcome any opportunity to participate in any implementation working groups for the telecommunications sector.

ATTACHMENT A

Domain Name System

Overview

The DNS is a distributed hierarchical database which contains a listing of domain names and various types of information about them. A domain name denotes an Internet Resource such as a website, an email server, a database server or any machine or service that is connected to the internet. Although the DNS has a variety of uses, the most important function of the DNS is to associate domain names with Internet Protocol (IP) addresses of the systems that host the Internet Resource. This allows users to access Internet Resources using memorable and recognizable names. The DNS creates a logical linkage between the domain name and Internet Resource, which ensures that the domain name stays the same even though the IP address of the host of that Internet Resource may change.

.au structure

The .au ccTLD is the Australian address book for Australian licensed domain names in the DNS hierarchy. The Internet Resources referenced by these domain names, such as websites, email servers, database servers, and any device connected to the Internet, can be and frequently are located outside of Australia. For example it is very common for Australians to host their websites in the USA, to take advantage of lower cost Internet capacity . The .au ccTLD is a hierarchically organized tree structure. The .au domain branches into special purpose second level domains (2LD), and the edu.au 2LD and the gov.au 2LD branch into third level domains (3LD) representing each State and Territory (Fig 1).

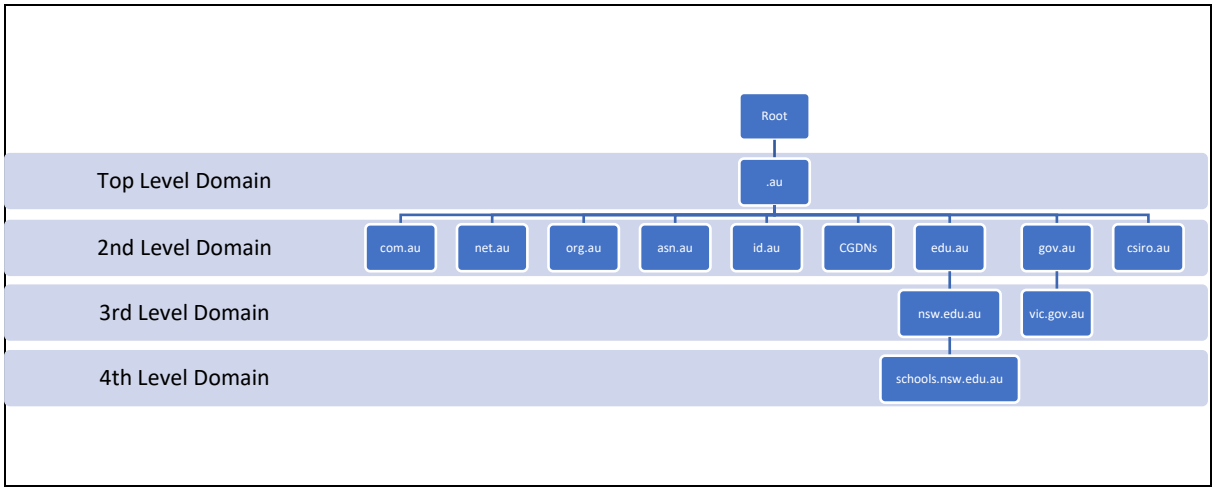


Figure 1: Structure of the .au ccTLD

Each 2LD and 3LD has a special purpose, which makes it easier for a person to identify the type of entity using the domain name and reduces consumer search costs (Table 1). The 2LDs are further categorized into:

(a) open 2LDs (com.au, net.au, org.au, asn.au and id.au) which allow any person to register a domain name, subject to satisfying the eligibility and allocation criteria for that 2LD.

(b) restrictive 2LDs are the State and Territory namespaces (vic.au, nsw.au, sa.au, tas.au, act.au, qld.au, nt.au and wa.au). Registration of domain names in the State and Territory 2LDs are restricted to community groups within the border of the

State or Territory to which the 2LD corresponds. The domain name used by the community must match the name of the geographical locale in which the community group resides.

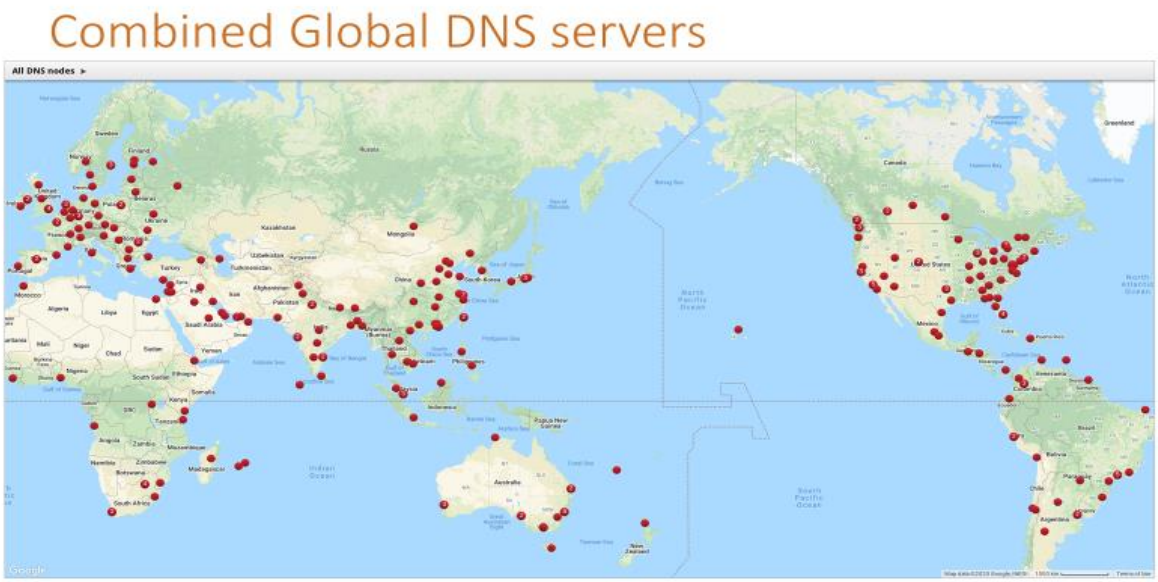
(c) closed 2LDs are the gov.au and edu.au 2LDs.

The gov.au 2LD comprises the State and Territory Government 3LDs (vic.gov.au, nsw.gov.au, qld.gov.au, nt.gov.au, wa.gov.au, sa.gov.au, act.gov.au and tas.gov.au). auDA has delegated administration of the gov.au 2LD and child zones to the Australian Government Digital Transformation Agency under the gov.au Sub-Sponsorship Agreement.

The edu.au zone comprises the State and Territory education 3LDs. A person can only register a domain name in the edu.au 2LD or State or Territory 3LD if it is a regulated education provider or a related service provider, such as university colleges. For example, all Victorian Government primary and secondary schools have their domain name registered in the vic.edu.au 3LD.

All domain names registered in the 2LDs and 3LDs are recorded in the Registry, except domains within csiro.au, and the tas.gov.au and nt.gov.au 3LD. These domains are managed by third party administrators, and the csiro.au, tas.gov.au and nt.gov.au domains in the Registry only contain a pointer to DNS nameservers that contain information about the sub-domains in these 3LDs.

The .au DNS database is distributed across a very large number of geographically dispersed DNS nameservers that are managed by auDA or by contracted third party providers (Map 1).



Map 1: Global .au DNS servers

Each DNS nameserver contains information relating to a subset of the DNS namespace and pointers to other nameservers that can point to other parts of the data base. For example, a gov.au nameserver will point to the vic.gov.au nameservers, which will point to the police.vic.gov.au nameservers, which will provide the IP addresses for the website and email servers associated with the domain name police.vic.gov.au.

DNS queries

A person will type a domain name (auda.org.au) into a web browser, the query will be sent to the local DNS resolver in the person's computer. If the DNS resolver has a locally cached copy of the domain name's IP address, then it passes the information back to the browser. However, if there is no cached record, then the computer will ask a DNS resolver for the domain name's IP address. The DNS resolver starts by querying a root DNS server for the IP addresses of the .au TLD nameservers. The DNS resolver will then ask a .au TLD DNS nameserver for the IP addresses of the org.au DNS nameservers. The DNS resolver will then ask an org.au DNS nameserver for the IP addresses of the auda.org.au DNS nameservers. Finally the DNS resolver will ask an auda.org.au DNS nameserver for the IP address of the www.auda.org.au web server, and passes it back to the browser, which then contacts the website host using the IP address (Fig 2).

DNS Service Providers

There are several parties that are involved in providing DNS services. The DNS database is maintained by the Registry operator. auDA outsources the .au Registry function to Afilias Australia Pty Ltd, who is contracted to provide registration services for registrars, authoritative DNS nameserver services, the WHOIS registration data directory services and registrar support services for the .au ccTLD.

A person cannot register a domain name directly with the Registry and must use an auDA Accredited Registrar. Registrars are required to meet the auDA Information Standard (ISS) for Accredited Registrars and pass an independent audit before they become an auDA accredited Registrar and are granted access to the Registry. auDA as part of the reforms of the .au Licensing Framework requires Registrars to adopt and maintain an effective "Information Security Management System" in compliance with ISO 27001 or adopt and maintain any other recognized framework or standard approved by auDA.[47] auDA also requires Registrars to implement prescribed minimum security controls,[48] which are based on the Australian Signals Directorate Essential Eight.

Internet Service Providers (ISPs) provide DNS resolution services to their subscribers to enable them to use the DNS system and Internet. ISP customers are reliant on whatever recursive DNS resolvers the ISP uses for basic internet connectivity, and loss of the recursive DNS server can cut off nearly all Internet access for ISP subscribers. An ISP customer is free to use another DNS resolver of their choice (e.g. Cloudflare and Google public DNS resolvers) at no charge, but few customers know how to change the default configuration of their software. On 2 August 2020, several Telstra nameservers failed to resolve leaving some Telstra customers without Internet access. [49]

[47] auDA Registrar Agreement, cl 15.1(b)(ii)-(iii) < https://www.auda.org.au/assets/Uploads/auDA-Registrar-Agreement-20200625.pdf>
[48] Ibid, cl15.3
[49] Sydney Morning Herald, Telstra backtracks on claim network was hit by cyber attack (2 August 2020)

1) Laptop asks Resolver (ISP/Corporate/Personal) "where is www.auda.org.au"
2) Resolver takes on the job and asks the root server "where is www.auda.org.au"
3) Root server responds "I don't know but I do know where .au is, go ask them and here is their IP address"
4) Resolver asks the .au Name Server "where is www.auda.org.au"
5) The .au Name Server responds "I don't know but I do know where org.au is, go ask them and here is their IP address"
6) Resolver asks the org.au Name Server "where is www.auda.org.au"
7)The org.au Name Server responds "I don't know but I do know where auda.org.au is, go ask them and here is their IP address"
8) Resolver asks the auda.org.au Name Server "where is www.auda.org.au"
9) The auda.org.au Name Server response "I know, its at 104.17.237.107"
10) Resolver passes the IP for www.auda.org.au back to the laptop
11) Laptop talks directly to the webserver via the IP address
12) The auda.org.au webserver responds directly to the end user laptop with the page requests

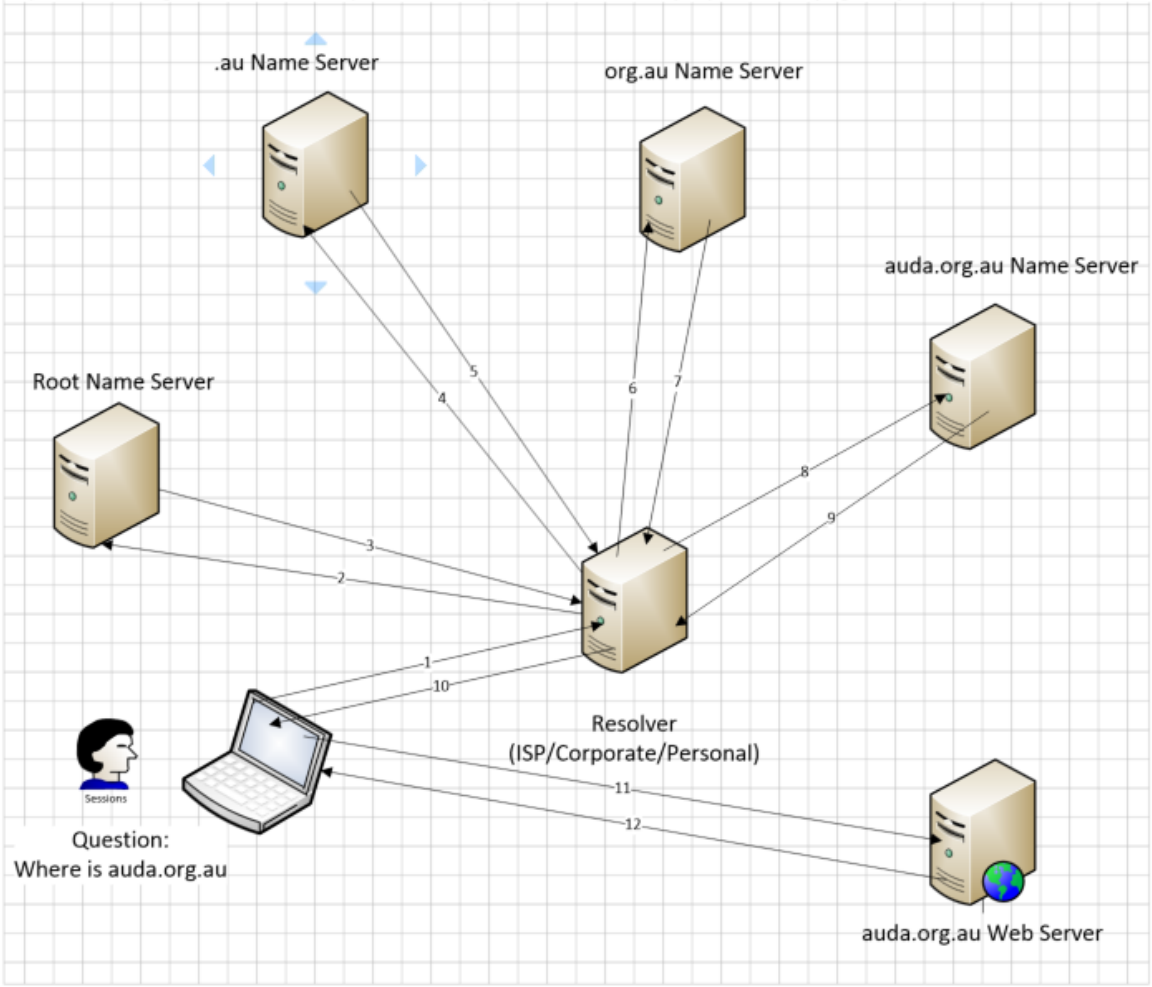


Figure 2: DNS queries

As the DNS is a network within a network, it relies on other internet and communications infrastructure, such as Internet Exchange Points, land based optical fibre, and submarine cables.