Building auDA 2.0

Enterprise Security Strategy

September 2018

.au DOMAIN ADMINISTRATION LTD

www.auda.org.au

PO Box 18315
Melbourne VIC 3001

info@auda.org.au

Table of Contents

1. Introduction

Under the auDA constitution, auDA's principal purposes include:

- To be the administrator of, and the Australian self-regulatory body for the *.au* ccTLD and its associated Second Level Domains
- To 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
- To manage the operation of critical technical functions including:
    - The primary and secondary *.au* name servers
    - Zone files for second level domains; and
    - A searchable database containing information on registration within the .au ccTLD

Under the Registry Transformation Project, project goals include:

- to become a world leader in managing security, confidentiality, integration and availability of au registry data, and
- to build a data science and data analytics capability in relation to the registry data.

auDA's enterprise security strategy is to implement worlds' best practice with respect to its information security management systems. Where possible auDA will identify and comply with key local and international standards, and use external auditors to provide independent confirmation that auDA is meeting those standards. auDA will also conduct regular external testing of the security of its systems, which will include both automated penetration testing as well as red team testing.

The following sections describe each component of the .au end-to-end domain name registration system, the core responsibilities, applicable standards, and planned deliverables.

2. .au eco-system

2.1 auDA (.au Domain Administration Limited)

Core IT system responsibilities:

- manages the *.au* top level domain zone and DNS name servers
- manages the auDA data repository – contains copies of the historical registry data (pre-June 2018), current registry data, log files, registry source code
- monitors all registry service levels – registration system, WHOIS and DNS
- responsible for business continuity in the event of registry failure
- manages membership information – including personal data of individuals
- manages compliance complaint information - including personal data of complainants

Applicable information security standards:

- ISO 31000 Risk management – Principles and Guidelines
- ASD Strategies to Mitigate Cyber Security Incidents (Essential eight)
- ISO 27001 – Information Technology – Security Techniques – Information Security Management Systems - Requirements
- ISO 22301 – Societal Security – Business Continuity Management Systems – Requirements

- ISO 20000 – Information Technology - Service Management – Service Management system requirements
- ITIL Service Operation – 2011 edition
- AS 4811 – Employment screening
- National Identity Proofing Guidelines (Level 3)

Planned deliverables in 2018-2019 financial year:

- Enhanced director and employee screening processing to comply with AS 4811 and conduct identity checks in accordance with the National Identity Proofing Guidelines (level 3) – Sept 2018
- Conduct automated penetration testing of auDA's key IT platforms – including .au DNS systems and auDA data repository – 2018
- Update ISO 27001 complaint Information Security Management System (ISMS) that can be mapped to the relevant components of the Australian Government's Information Security Manual – Dec 2018
- Incorporate compliance with the ASD Strategies to Mitigate Cyber Security Incidents also known as the *Essential Eight* into the ISMS – Dec 2018
- Form a *Technical Advisory Standing Committee* – comprising a combination of auDA members, stakeholders and other interested parties - Dec 2018
- Conduct red-team penetration testing of auDA's key IT platforms – 2019
- Work with the Australian Government on ensuring some staff have the Government security clearances required to receive briefings on matters of national security – Mar 2019
- Update auDA's Business Continuity Management Systems (BCMS) to be ISO 22301 complaint, including running a disaster recovery test for the failure of the Afilias registry at least annually – Mar 2019
- Based on international best-practice, further reform of auDA's security and risk processes to ensure continued monitoring and improvement, including consideration of service management (SMS) best practice in ISO 20000 - ongoing

2.2 Registry Operator (Afilias Australia Pty Ltd)

Core IT system responsibilities:

- manages the second level domain zones (including com.au, net.au, org.au, gov.au, edu.au, id.au, asn.au, vic.au, nsw.au, act.au, tas.au, qld.au, nt.au, wa.au, sa.au) and DNS name servers
- manages the domain name registry – incorporating information on the domain name registrants and DNS settings
- provides the WHOIS directory service
- provides IT service provider tools – such as domain check, and password recovery

Applicable information security standards:

- ISO 31000 Risk management – Principles and Guidelines
- ASD Strategies to Mitigate Cyber Security Incidents (Essential eight)
- ISO 27001 – Information Technology – Security Techniques – Information Security Management Systems - Requirements
- ISO 22301 – Societal Security – Business Continuity Management Systems – Requirements
- AS 4811 – Employment screening
- National Identity Proofing Guidelines (Level 3)

Planned deliverables in 2018-2019 financial year:

- Conduct red-team penetration testing of Afilias' key IT platforms – Dec 2018
- Ongoing monitoring of performance against the auDA-Afilias registry agreement – including approvals of changes to key personnel, and any changes in subcontractors (such as data centre providers)
- Participate in disaster recovery test for the failure of the Afilias registry at least annually – Mar 2019

2.3 Registrars

Core IT system responsibilities:

- Collect registrant and DNS information associated with domain names
- Provide registrant and DNS information to the registry for publishing via the DNS and WHOIS services

Applicable information security standards:

- 2013-03 – auDA Information Security Standard (ISS) for Accredited Registrars
- ASD Strategies to Mitigate Cyber Security Incidents (Essential eight)
- ISO 27001 – Information Technology – Security Techniques – Information Security Management Systems - Requirements

Planned deliverables in 2018-2019 financial year:

- Review of auDA's Information Security Standard (ISS) for accredited registrars. The review will consider the option of using the ISO 27001 ISM Framework, incorporate the ASD Essential Eight, and review which controls from the Australian Government's Information Security Manual (ISM) should be made mandatory – June 2019.
- Conduct penetration testing of Registrar systems – ongoing.
- Assist the Digital Transformation Agency to improve security of *gov.au* – including using DNSSEC to secure *gov.au* and *csiro.au* - ongoing

2.4 Resellers

Core IT system responsibilities:

- Collect registrant and DNS information associated with domain names
- Provide registrant and DNS information to registrars for passing on to the registry

Applicable information security standards:

- ASD Strategies to Mitigate Cyber Security Incidents (Essential eight)

Planned deliverables in 2018-2019 financial year:

- Encourage resellers to implement the ASD Strategies to Mitigate Cyber Security Incidents (Essential eight) - ongoing

3. Collaboration with external organizations

auDA will collaborate with and where possible participate in the following technical and security groups :

- ICANN's Security and Stability Advisory Committee (SSAC)
    - Attend public meetings
    - Share information

  - Formally review SSAC advice, once it is published, for relevance to .au
- Domain Name System Operations Analysis and Research Center (DNS-OARC)
  - Attend public meetings
  - Share information
- Council of European National Top-level Domain Registries (CENTR)
  - Associate member
  - Attend public meetings
  - Share information
- Internet Engineering Task Force (IETF)
  - Attend meetings of the Domain Name System Operations (dnsop) working group
  - Participate in the DNS related mailing lists
- Asia-Pacific Network Information Centre (APNIC)
  - Collaborate on the development of training materials around DNS and IP addressing
- Internet NZ
  - Joint-meetings
  - Share information about security incidents

4. Collaboration with the Australian Government

auDA will collaborate with and exchange information with the following Australian Government agencies

- Australian Signals Directorate (ASD)
  - Seek guidance on choices of hardware and software that meet ASD security standards
  - Engage in scenario exercises
  - Seek guidance on scope of work for penetration testing
- CERT Australia
  - Subscribe to security alerts
  - Share information on security incidents
- Australian Cyber Security Centre (ACSC)
  - Follow publicly available information on strategies to reduce cyber security incidents, and evaluated products list
- Joint Cyber Security Centre (JCSC) – Melbourne
  - Participate in local activities of the JCSC
  - Provide briefings on best practice DNS management
- Australian Federal Police (AFP)
  - Share information on trends in domain related complaints
  - Training on what to look for with domain names and IP addresses
  - Respond to formal requests for information
- Critical Infrastructure Centre, Department of Home Affairs
  - Follow and contribute to the development of cyber security policy
  - Seek guidance on choices of hardware and software vendors, and IT service providers