Inquiry into the capability of law enforcement to respond to cybercrime

January 2024

.auDA

Contents

About auDA

The .au Domain Administration Limited (auDA) is auDA is the not-for-profit organisation endorsed by the Australian Government to administer the .au country code Top Level Domain (ccTLD) for the benefit of all Australians.

The .au ccTLD is part of Australia's critical infrastructure, supporting more than 4 million .au domain names. 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.

In performing its functions, auDA operates under a multi-stakeholder model, working closely with suppliers, business users, industry, civil society, 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 is part of a global community of organisations in the domain name industry and engaged in internet governance. It 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).

auDA's role

As the operator of Australia's domain name system, forming part of Australia's critical infrastructure as defined in the *Security of Critical Infrastructure Act 2018 (Cth)*, 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 appropriate compliance and dispute resolution processes associated with the licensing rules
- appoints the .au registry operator and accredits and licenses registrars
- advocates for, and actively participates in, multi-stakeholder internet governance processes both domestically and internationally.

To find out more about auDA, visit www.auda.org.au.

Submission

auDA appreciates the opportunity to provide input into the inquiry into the capability of law enforcement to respond to cybercrime.

auDA regularly engages with Commonwealth, state and territory government agencies, including law enforcement agencies, regulators, consumer affairs and fair-trading bodies to keep the .au ccTLD trusted and secure.

In accordance with our Licensing Rules, we can take action to uphold the technical integrity of the .au ccTLD. We are not, however, authorised to act in relation to content hosted on websites accessed via a .au domain name. Matters relating to inappropriate or harmful online content are managed by relevant regulatory bodies including the eSafety Commissioner and the Australian Communications and Media Authority (ACMA).

auDA recognises the importance of law enforcement agencies having the capacity to detect, investigate and prosecute cybercrime, and we offer the following comments against the terms of reference. We would be happy to elaborate on these comments if the committee would find it helpful.

Existing law enforcement capabilities in the detection, investigation and prosecution of cybercrime, including both cyber-dependent and cyber-enabled crimes

With the exception of a small number of specialist areas within the Australian Federal Police (AFP), there does not appear to be a deep understanding within law enforcement bodies, as to the internet ecosystem. This lack of clarity extends to a lack of awareness about the roles and responsibilities of the various actors in the ecosystem, including telecommunications companies, internet service providers, web hosting companies, email service providers, cloud computing operators, domain name system (DNS) operators, registrars and web developers.

auDA suggests targeted training on the internet ecosystem and the actors within it would enhance the detection and investigation of cybercrime by ensuring that requests for assistance are directed to the most appropriate entity.

There is also a low level of understanding about the different Top-Level Domains (TLDs). There are over 1500 TLDs globally, operated by numerous public and private entities. As the administrator of the .au ccTLD, auDA is able to assist with enquiries related solely to domain names ending in .au. auDA is not responsible for the administration of other TLDs and is unable to respond to enquiries related to them.

Ensuring a trusted and secure .au

The .au Licensing Rules keep the .au domain secure and trusted and reduce the risk of abusive registrations and harm to the community. auDA works closely with registrars accredited to register .au domain licences to ensure those who register a .au domain name licence have an Australian presence and meet the relevant .au eligibility and allocation criteria. We require our accredited registrars to validate a registrant's details when they register, renew or transfer a domain name licence.

Where registrants do not meet the requirements of the .au Licensing Rules, their licence may be suspended or cancelled.

Where a .au domain name poses a risk to the security, stability or integrity of the .au domain, we can take immediate action to suspend or cancel the .au domain name licence. auDA undertakes regular audits of registered .au domain names to ensure compliance with our rules.

auDA makes selected domain name licence information publicly available through the .au WHOIS tool (tool). The tool is an essential element of online accountability that allows law enforcement agencies as well as the community to check which legal entity and type of legal entity has registered a domain name.

auDA suggests that greater awareness of the public WHOIS and other publicly available tools that help people find information about domain name registrations may assist law enforcement officers investigating crimes. Information on some of these tools is below.

Public tools for identifying domain registration information

The .au WHOIS tool allows anyone to query a domain name and find the identity and contact details of a .au domain name registrant. The .au WHOIS is available at https://whois.auda.org.au/. It provides the following information:

- **Registrar:** registrar of record for the domain name
- **Registrant and Registrant ID:** the legal name of the registrant of the domain name, along with their Government-issued identifier (such as an ABN, ACN, or state-based incorporation number)
- **Eligibility Type:** type of legal entity of the registrant (such as sole trader, company, incorporated association, or Trust)
- **Eligibility Name and Eligibility ID:** the business name or trademark of the registrant, along with the relevant Government-issued identifier (such as an ABN or Australian Trademark number)
- Registrant contact name and email address
- Technical contact name and email address
- DNS servers for the domain name.
- **Status:** domain name status information (such as whether it is ready for renewal, expired, or scheduled for deletion)

Telephone numbers and postal addresses related to .au domain names are not publicly available via the .au WHOIS, but can be requested by law enforcement under the provisions of the Privacy Act.

The .au WHOIS is only for information about domain names within the .au ccTLD. For domain names in other TLDs, the Internet Corporation for Assigned Names and Numbers offers a domain registration data tool, which can be found at https://lookup.icann.org/en

Another tool that law enforcement officers may find helpful in investigating crimes is the Abuse Contact Identification Tool. This tool, provided by ICAN's Registrar Stakeholder Group, allows users to enter a domain name into a search bar and find the public contact information for web hosting, email, and domain registration providers associated with that domain name. It is available at https://acidtool.com/

International, federal and jurisdictional coordination law enforcement mechanisms to investigate cybercrimes and share information related to emerging threats

auDA notes that the second additional protocol to the Budapest Convention on Cybercrime allows competent authorities in one party's jurisdiction to make direct requests for domain registration data to entities in another party's jurisdiction.

auDA's current practice is to refer any requests for information from foreign law enforcement officers to our public .au WHOIS tool. Any requests for information outside this scope will be directed to the AFP.

We understand the Budapest Convention second additional protocol does not compel registries or registrars to provide non-public information to foreign officials, and that parties to an international treaty retain the right to determine how treaty obligations are implemented in their own jurisdiction.

We understand that a decision as to whether Australia will accede to the additional protocol will not take place until negotiations on the United Nations cybercrime treaty have concluded (scheduled in late 2024).

auDA would be pleased to engage in any consultation processes relating to these treaties at the appropriate time, however, we take this opportunity to recommend that should Australia accede to the additional protocol, any requests from a foreign authority for non-public .au domain registration information should come via an appropriate Australian authority, such as the AFP.

While we recognise that timeliness is critical during cybercrime investigations, and that mutual legal assistance treaties can have significant limitations in this regard, we consider that any potential risks associated with providing non-public information to foreign governments should not be borne by private companies.

We acknowledge the willingness of officials from the Attorney-General's Department and the Department of Foreign Affairs and Trade to engage with auDA during the development of this treaty, and we look forward to providing further input to consultation processes at the appropriate time.

Summary

auDA recognises the need for law enforcement officers to be able to detect, investigate and prosecute cybercrime in a timely manner. We regularly engage with Commonwealth, state and territory government agencies, including law enforcement agencies, to keep the .au ccTLD trusted and secure.

We suggest law enforcement officers would be supported in this task by developing a greater understanding of the internet ecosystem. We also suggest greater awareness of existing publicly available tools related to domain name registrations and DNS abuse would assist law enforcement officers in their investigations.

auDA's current practice is to direct any requests from foreign law enforcement agencies to the public .au WHOIS tool. Any request for information that is not publicly available should be made via the AFP. auDA recommends that implementation within Australia of any international treaty should direct requests for data from foreign governments to the appropriate Australian officials.

auDA would be pleased to further discuss any of the information in this submission. Please contact auDA's Internet Governance and Policy Director, at or .

.au Domain Administration Ltd
www.auda.org.au

PO Box 18315
Melbourne VIC 3001
Contact information: https://www.auda.org.au/about-auda/contact-us

January 2024