

13 October 2025

Committee Secretary  
Parliamentary Joint Committee on Law Enforcement  
PO Box 6100  
Parliament House  
Canberra ACT 2600

## Submission to the *Inquiry into combatting crime as a service*

auDA is pleased to contribute to [the \*Inquiry into combatting crime as a service\*](#) (the Inquiry), initiated by the Joint Parliamentary Committee on Law Enforcement on 4 September 2025.

In this brief submission, auDA provides information from its recent research findings relevant to the Inquiry, and explains how it works with law enforcement. We trust this will assist the Committee with the Inquiry.

### About auDA

[The .au Domain Administration Limited](#) (auDA) is the trusted administrator of the .au country code Top Level Domain (ccTLD). As a critical part of the digital economy, auDA's role is to ensure the .au ccTLD remains stable, reliable and secure.

More information about auDA is available as **Appendix 1: about auDA**.

### Research findings

auDA conducts regular research into the *Digital Lives of Australians*. In the [2025 report](#), the following key findings relate to the Inquiry's Terms of Reference:

#### **Australians' concerns about cybersecurity inhibits their online activity**

A vast majority of Australians believe cybercriminals are becoming more sophisticated (83 per cent) and are so concerned they actively avoid certain online activities (67 per cent). However, in parallel, many business and government services are now only available online. In the long-term, avoiding key online activities will limit our ability to benefit from digital technologies.



### **Small businesses are vulnerable and need to change their approach**

Unfortunately, the majority of Australian small businesses are greatly underprepared. Only one in five (20 per cent) small businesses have a formal cyber security policy or offer staff training, a decrease from 2021, and less than a quarter (21 per cent) do not spend any money on cyber security.

Small businesses are the backbone of Australia's economy and this preparedness gap is a vulnerability we cannot afford to ignore. We need to foster an environment where businesses, regardless of size, are equipped with the skills and resources to protect themselves, their staff and their customers.

### **Skills development is a key part of the response**

Cyber security isn't just about technology, it's also about people. The skills gap is a barrier to confidence. While most Australians (69 per cent) consider cyber security to be an important digital skill for the future, only a small minority feel they have high capability (17 per cent of working men and 10 per cent of working women).

Our research also reveals a gender gap, with 72 per cent of women believing they lack the technical skills for a career in IT, compared to just 54 per cent of men. Yet, a majority of Australians (57 per cent of women and 48 per cent of men) recognise that diversity brings value to the IT industry through improved innovation and problem-solving.

To improve the digital lives of all Australians, we must invest in building digital literacy from the ground up. This means working collaboratively across industry government and academia to create trustworthy resources, empower communities with tailored training and encourage a pipeline of talent, including underrepresented groups, to develop a nation of cyber-smart citizens.

### **A collective effort is required**

No single actor can improve Australia's resilience to cyber security risks. Every category of stakeholder has a role. Government is stepping up through its work in the cyber security strategy. Seeing that work through and encouraging all stakeholders to do what they can is vital.

## **Securing the .au domain name space**

auDA's core function is the secure operation of the .au domain.

The domain name system (DNS) is one way that crime-as-a-service can be propagated, through what is often termed "DNS abuse". This involves people using the



DNS to enable malicious activity, for example through using a domain name that is a slightly misspelling of the legitimate website or email address.

DNS abuse is a global problem, but is at a low rate in the .au domain for which auDA is the steward. This low local incidence is due to auDA's proactive compliance posture, and due to the licensing obligations that apply to people holding .au domain names. These are core components of our broader role in keeping .au secure.

The connection to the concept of crime as a service emerges most clearly in small business websites that haven't kept their software or infrastructure up to date. This can see their websites compromised and used to, for example, host fake online shops, or other forms of scam.

Where auDA becomes aware of such compromised websites, it works with the domain name license holder to help them mitigate the problem. For example, this may involve suggesting the license holder work with the hosting provider or the company that built the website to update relevant software, remove compromised access to the service, and so on.

If it is of interest, further information about auDA's work securing the .au domain is available in our [A secure .au](#) report. Details about [how auDA engages with Australian enforcement agencies](#) are also available.

If the Committee wishes to call auDA as a witness, or seeks any further information, please contact [REDACTED]

Thank you for considering the information in this submission.

Yours faithfully

**Dr Bruce Tonkin**  
**Chief Executive Officer**



## Appendix 1: About auDA

The .au Domain Administration Limited ([auDA](#)) is the trusted administrator of the .au country code Top Level Domain (ccTLD). The .au ccTLD is part of Australia's critical communications infrastructure, supporting more than 4.2 million .au domain names. auDA is endorsed by the Australian Government to administer the .au for the benefit of all Australians under its [Terms of Endorsement](#).

As a critical part of the digital economy, auDA's role is to ensure the .au ccTLD remains stable, reliable and secure. Additionally, auDA performs the following functions:

- Administering a licensing regime for .au domain names based in multi-stakeholder processes, including:
  - Developing policies for the .au domain with a multi-stakeholder approach to provide the greatest benefit for the Australian community
  - Managing enquiries from the public about the .au Licensing Rules
  - Maintaining an appropriate compliance and dispute resolution process associated with the .au Licensing Rules
  - Making limited information available on the holder of a domain name licence through a publicly accessible tool at <https://whois.auda.org.au/> (a standard feature of domain name systems around the world and an essential element of online accountability)
- Accrediting registrars to provide domain name registration services to the Australian internet community
- Advocating for, and actively participating in, multi-stakeholder internet governance processes both domestically and internationally.

In performing its functions, auDA operates under a multi-stakeholder model, working closely with the technical community, suppliers, business users, industry, civil society, consumers and the Australian Government.