18 October 2025

Input on the Preliminary Issues Report on a Policy Development Process on DNS Abuse Mitigation

auDA is pleased to contribute input in response to the Preliminary Issues Report on a Policy Development Process (PDP) on DNS abuse mitigation, published for public comments on 8 September 2025.

In this brief submission, auDA outlines its approach to mitigating domain name system (DNS) abuse. We share lessons learned in taking this approach which we hope will be helpful in informing decisions about the next steps for this PDP.

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.

auDA's approach drives low DNS abuse in .au

auDA maintains robust rules for .au domain names that support the integrity of the .au domain. It also maintains a rigorous compliance posture to ensure the rules are followed.

Key facets of the rules include:

- Requiring registrants to have an Australian presence
- A .au Dispute Resolution Policy (auDRP) to address competing legal rights to a .au domain name.

Our compliance approach includes:

- Mandatory validation of registrant eligibility by .au registrars – at registration, renewal and transfer
- Complaint handling processes with several points of review

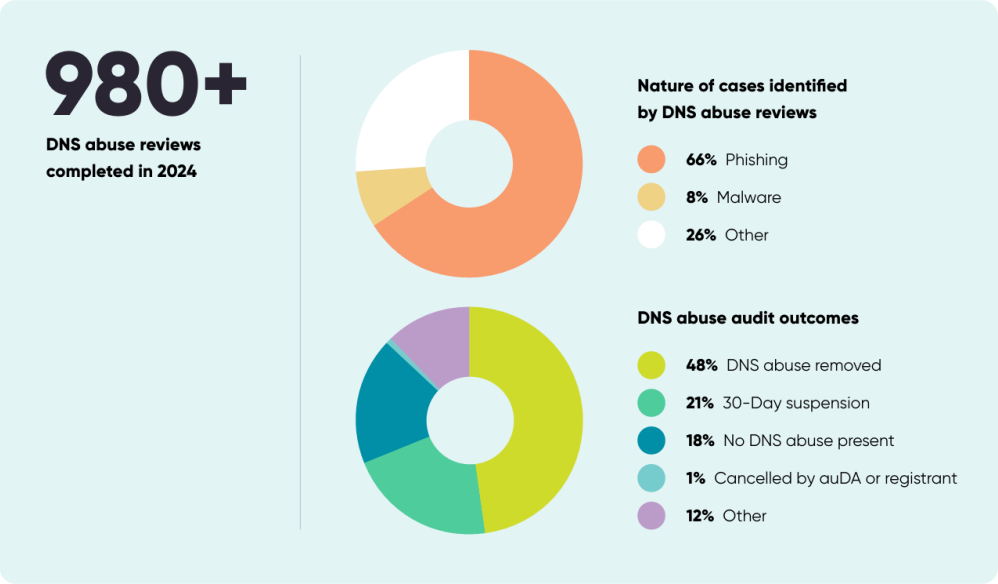
- Suspension and cancellation of .au licences when false registration information is provided
- A proactive audit program to verify compliance with the rules, including initiating a review within one business day where DNS abuse is identified
- Daily monitoring of 25+ threat feeds to identify suspected DNS abuse
- Working with enforcement bodies when they make requests under their legal remit.

auDA collaborates with groups including the NetBeacon Institute, the Country Code Names Supporting Organisation's DNS Abuse Standing Committee, Asia Pacific Top Level Domain association and the Pacific ccTLD forum to learn and share best practice on these matters.

These elements of auDA's approach have delivered very low levels of DNS abuse, as set out in auDA's *2025 A secure .au* report:

- 0.0002% of .au domain names had an instance of DNS abuse (at December 2024)
- 1.31 cases of DNS abuse per 100,000 domains under management at January 2025 (down from 2.22 in January 2023).

The following infographic shows the nature and outcomes from DNS abuse reviews completed during 2024:



For further information on auDA's approach and for citations relating to statistics in this section, please refer to auDA's *A secure .au* report, published in May 2025.

The Preliminary Issues Report

On the Preliminary issues report, auDA commends the work by NetBeacon and the GNSO's DNS Abuse Small Team that have led to the report.

auDA supports a PDP being launched on the issues suggested, and accepts the logic of splitting the issues into an initial tranche of work, with subsequent work to be determined later (as outlined in section 3.2 (p. 39)).

All the issues listed in section 3.2 should eventually be addressed, to strengthen efforts to mitigate DNS abuse in the gTLD space.

auDA offers the following specific comments on the two areas proposed for this PDP.

1) Unrestricted Application Programming Interface (API) access for domain name registration for new customers

auDA observations:

From the data that auDA sees for .au, the use of APIs is most common with registrars that have a reseller business model.

The hypothesis is that some registrars allow resellers to be signed up through click-through agreements and the provision of some form of payment - e.g. a credit card. auDA believes that it is possible to register many domain names for malicious purposes using these reseller accounts.

auDA mitigations:

auDA monitors spikes of registrations that have common elements on a daily basis - e.g. spikes of registrations with common registrant information - and investigates those that looks suspicious.

auDA will contact the registrar to request additional validation from the registrant such as official company registration documents. auDA will suspend and ultimately cancel registrations that appear to have been registered with false registrant information.

auDA requires potential registrars to have operated as a reseller for 6 months with a history of valid registrations before accrediting a new registrar.

Potential solutions:

auDA supports the NetBeacon proposal to introduce proportionate, risk-based friction to the process of signing up for reseller accounts with API access. Possible approaches could include:

- Additional validation for reseller accounts that have API access - this could include requiring additional documents and phone validation - essentially better know your customer (KYC) procedures appropriate for accounts with API access
- Initially setting limits on how many registrations can be made within an hour or over a 24 hour period - similar to the approach to rate-limit WHOIS access
- Ensure that bulk registrations must be paid for in advance, potentially through bank transfers rather than just credit cards (which may be stolen, and subject to charge backs)
- Potentially limit access to APIs for new reseller accounts for a period - e.g. 30 days, and require web-based registration with appropriate **CAPTCHA** protections. Once a history of valid web-based registrations has been established with appropriate verified payment, then open up API access.

(2) Associated Domain Checks

auDA observations:

Often when auDA receives reports of DNS abuse, there are other related domains that have been registered in .au. In terms of DNS abuse reports, we often get reports of domain names associated with websites that have been compromised. We see cases where there are multiple compromised websites that may have been associated with a particular web server that has many clients that are sharing a common version of unpatched software.

Sometimes web developers focus on removing the web pages that have been compromised, and then the website gets compromised again a few months later. The preferred solution is to review all the websites that may have been on a compromised server, remove the offending content, and then upgrade the software version that is

vulnerable so that it doesn't get compromised again.

auDA mitigations:

When auDA receives a valid report of DNS abuse, it will look for other domain names that have been registered with similar registrant information.

auDA will also look at patterns of domain names that might be related to a particular form of financial scam, and search the registry database using related key words. For example, where domain names have been registered with false information for the purposes of creating fake shops (where a person pays a significant amount of money for a product that is never delivered) to sell high value items like shipping containers, auDA will look for domain names that include common keywords like shipping or container.

Where auDA suspects that a domain name has been registered with false information, auDA will contact the registrar to request additional validation from the registrant such as official company registration documents.

Where auDA suspects that a domain name is associated with a compromised website, auDA will notify both the registrar and the registrant to investigate the content issue, remove the offending content, and upgrade the software on the website to prevent it happening again.

Potential solutions:

auDA supports the NetBeacon proposal to require an associated domain name check that requires registrars to proactively investigate other domains registered by a particular registrant or account when DNS abuse is identified on one of their other domains.

At the registry level we can investigate domain names with related information to those domain names that have been registered with false information, but we do not have visibility of the domain names that may be registered through a registrant or reseller account at the registrar.

The policy should require registrars to investigate at the level of both the registrant and (where applicable) the reseller account. With respect to resellers that are hosting companies or web developers, registrars should advise the resellers to review other domains that are sharing a common webserver software environment, to investigate

whether updating or patching the website software can reduce the risks for other customers.

In closing, auDA notes that development in the ICANN context of further DNS abuse mitigations through open means such as this PDP is important. While the contractual negotiations that led to revised registry and registrar contracts in 2024 improved the tools for mitigation of DNS abuse, it is important to prove that multi-stakeholder processes can also achieve improved tools. This PDP offers the GNSO the opportunity to demonstrate this, and in doing so, strengthening the overall reputation of ICANN's multi-stakeholder model and its effectiveness in tackling important challenges.

For any further information, please contact Jordan Carter, Internet Governance and Policy Director, on Jordan.Carter@auda.org.au or +61417243647.

Yours faithfully

Dr Bruce Tonkin
Chief Executive Officer