14 February 2025

Internet Governance area
Department of Infrastructure, Transport, Regional Development, Communications and the Arts
internetgovernance@communications.gov.au

Dear Sir/Madam

Re: Inquiry into .au Domain Administration Terms of Endorsement

CSIRO welcomes the opportunity to provide input into the review of the .au Domain Administration (auDA) Terms of Endorsement.

As Australia's national science agency, we play a trusted advisor role to community, industry and government in a range of areas including cybersecurity. As part of this, we administer the csiro.au website and domain as well as other web resources related to CSIRO's functions.

We provide the following input for the consideration of the review team, given our experience with domains and cybersecurity.

Domain Name System Security Extensions DNSSEC
The 2025 auDA Terms of Endorsement Review does not explicitly mention Domain Name System Security Extensions (DNSSEC). However, previous documents, such as the 2018 Review of the .au Domain Administration, highlight that auDA has implemented DNSSEC to enhance security by digitally signing data to ensure its integrity. Given the absence of DNSSEC in the current proposal, CSIRO would seek clarification on auDA's ongoing commitment to DNSSEC and other security measures. Ensuring that these protocols remain a priority is essential for maintaining the security and stability of the .au domain space.

Post-Quantum Safe DNS
Quantum computing threats could break RSA- and ECC-based cryptographic methods, making current DNSSEC implementations insecure in the future. No mention of post-quantum cryptography (PQC) transition in the auDA proposal raises concerns about the long-term viability of its security framework. Current industry efforts (such as NIST's post-quantum cryptography standardization) indicate that DNSSEC will require upgrades to use PQ-safe algorithms, but there is no clear transition plan for registrars or domain operators.
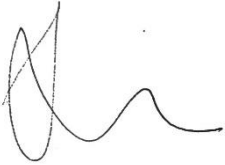
auDA should introduce a roadmap for post-quantum secure DNS that includes:
- Support for hybrid cryptographic approaches (for example PQC + traditional cryptography during the transition phase)

CSIRO
Australia's National Science Agency

- Guidelines for registrars and hosting providers to begin testing and adopting post-quantum cryptographic algorithms
- Coordination with international bodies (ICANN, IETF, NIST) to ensure alignment with global security standards
- Ensuring auDA mandates research and investment into post-quantum DNS security to prevent the .au domain space from becoming vulnerable to quantum attacks in the coming years.

We would be pleased to provide further detail on the input provided in this submission. For more information, please contact GovernmentRelations@csiro.au.

Yours sincerely

Jon Smith
Chief Information Officer
Jon.smith@csiro.au
+61 8 6436 8888