Digital Economy Council of Australia

Digital Economy Council of Australia

Submission to Department of Home Affairs

Date: 28 January 2026

2026 Reforms to the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act)

About DECA

As the peak industry body for Australia's blockchain, digital asset, AI, and Web3 sectors, the Digital Economy Council of Australia (DECA) champions responsible innovation. We collaborate closely with government bodies and regulators to establish frameworks that ensure Australia remains a globally competitive leader in the digital economy. DECA gratefully acknowledges the valuable insights provided by our members in shaping this response.

For further inquiries please contact:

- Amy-Rose Goodey, CEO – amy-rose@deca.org.au
- Alec O'Sullivan, Head of Operations – alec@deca.org.au

1. Issue: Scope of the Prohibition Power

Key Point

The power to prohibit products should be limited to registrable designated services to prevent regulatory overreach.

Response

DECA strongly advocates that the power be limited to **registrable designated services**. Broadening this power to *all* designated services risks capturing emerging technologies and broader economic activities that are not the primary focus of AML/CTF risks.

Commentary

Entities providing registrable services (like DCEs and remitters) are already subject to oversight and are best positioned to manage risk. Applying this power too broadly could inadvertently stifle innovation in non-financial sectors leveraging blockchain technology. International standards such as the FATF Recommendations emphasize a risk-based approach that targets specific higher-risk activities rather than broad technological categories.[1]

2. Issue: Management of "High-Risk" Technologies

Key Point

Risks arise from anonymity, but "difficulty" in mitigation often stems from a lack of **regulatory clarity** rather than the technology itself.

Response

[1] Financial Action Task Force (FATF), *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (Oct 2021), p. 23.

DECA posits that **no specific technology class** is inherently "unmanageable." Risks primarily arise from **anonymity-enhancing technologies** designed specifically to obfuscate illicit flows (e.g., non-compliant offshore mixers), rather than legitimate privacy tools.

Commentary

It is critical to distinguish between channels that are genuinely opaque and those that are merely novel. For example, fixed-location services (such as cash-to-digital asset infrastructure) are highly observable, attributable, and capable of generating structured intelligence. Conflating these controllable environments with "unmanageable" risks diverts regulatory attention away from truly opaque channels where harm is difficult to detect. For example, the Monetary Authority of Singapore (MAS) has successfully targeted specific high-risk consumer behaviors (like credit card leverage for crypto) without banning the underlying technology itself.[2] We urge the Department to distinguish between tools designed for crime and tools designed for privacy that can be regulated.

3. Issue: Criteria for Exercising Power

Key Point

Prohibitions must be a measure of **last resort**, subject to a strict public interest and economic impact test.

Response

The legislation must require the CEO to demonstrate that the risk **cannot be mitigated through existing AML/CTF controls** (such as enhanced due diligence or specific licence conditions) before a prohibition is issued.

Commentary

[2] Monetary Authority of Singapore (MAS), *Guidelines on Provision of Digital Payment Token Services to the Public* (Jan 2022).

A "public interest" test must be mandatory and explicitly include the **economic impact on competition and innovation**. We point to the UK's FCA, which conducted a detailed cost-benefit analysis before prohibiting crypto-derivatives for retail clients, explicitly considering consumer harm versus market impact.[3] Without such criteria, the power risks becoming a tool for "de-banking by regulation."

4. Issue: Procedural Fairness and Oversight

Key Point

Parliamentary oversight is essential; consultation periods must be **statutory minimums**.

Response

DECA supports the use of a legislative instrument to ensure parliamentary oversight. However, we strongly recommend that the **30-day consultation period be a statutory minimum** that cannot be waived except in verified national security emergencies.

Commentary

The explanatory statement accompanying any instrument must detail **why existing powers** were deemed insufficient. This aligns with the US Treasury's Section 311 "special measures," which typically require a Notice of Proposed Rulemaking to ensure due process and industry input.[4]

5. Issue: Safeguards and Due Process

Key Point

[3] Financial Conduct Authority (UK), *PS20/10: Prohibiting the sale to retail clients of investment products that reference cryptoassets* (Oct 2020), p. 5.
[4] U.S. Department of the Treasury, Financial Crimes Enforcement Network, *Section 311 Special Measures*.

Safeguards are needed to prevent permanent prohibitions without review.

Response

We propose three specific safeguards: **Sunset Clauses** for urgent prohibitions (expiring after 3 months), a published **Statement of Reasons**, and access to **Merits Review**.

Commentary

Decisions of this magnitude can destroy businesses overnight. "Urgent" prohibitions made without consultation should expire automatically unless ratified by a full process, similar to the temporary product intervention powers granted to ESMA under MiFIR Article 40.[5] It is a common misconception that all AUSTRAC powers are automatically subject to review; they are not. Merits review is essential given the potential for severe commercial damage based on administrative decisions.

6. Issue: Definition of Future Risk

Key Point

The proposed model is **too broad** and risks capturing benign innovation as "high-risk."

Response

DECA is concerned the model allows prohibitions based on "likely" harm, which is a low threshold for emerging tech. We recommend AUSTRAC establish a **technical advisory committee** with industry experts to assess whether a product is truly "high-risk" or simply "novel."

[5] European Securities and Markets Authority (ESMA), *Product Intervention Powers under MiFIR Article 40*.

Commentary

This consultative approach ensures Australia does not prematurely stifle innovation that other jurisdictions, like the EU under MiCA, are seeking to regulate rather than ban.[6] A technical committee would provide the necessary nuance to distinguish between structural flaws and manageable risks.

7. Issue: Criminal Liability Standards

Key Point

Penalties are proportionate but must require **intent**.

Response

The proposed maximum penalty (2 years imprisonment / 500 penalty units) appears proportionate. However, liability should only attach where the entity has **knowingly** or **recklessly** continued the service.

Commentary

In a decentralized global network, inadvertent interaction (e.g., via smart contracts or open protocols) should not automatically trigger criminal liability without intent. Strict liability in this context could make compliance impossible for automated systems.

8. Issue: Legislative Alignment (Terrorism Financing)

Key Point

DECA supports the **technical alignment** to include state sponsors of terrorism.

[6] European Parliament and Council, *Regulation (EU) 2023/1114 (Markets in Crypto-Assets Regulation)*, Art. 103.

Response

DECA supports the technical alignment with the *Criminal Code* and *Charter of the United Nations Act* to include state sponsors of terrorism. We have no objection to the inclusion of offences against section 112.5 and Division 113 of the Criminal Code.

Commentary

This is a logical extension of the existing framework and closes a gap regarding state-based actors.

9. Issue: Operational Implementation

Key Point

Operational impact will require new guidance on **"State-Linked" indicators**.

Response

While the amendment is consequential, it will require digital asset exchanges to update transaction monitoring systems. We request AUSTRAC provide **specific indicators or typologies** relevant to **state-sponsored terrorism financing via crypto-assets**.

Commentary

Identifying state-linked actors in decentralized networks is significantly more complex than identifying individuals. We welcome the Department's confirmation that the Travel Rule will commence on 1 July 2026 to allow for systems preparation. We submit that a similar transition period should apply to these new terrorism financing definitions, ensuring reporting entities have sufficient time to ingest new typologies and update monitoring rules without causing disruption.