

Submission: Drone Security Public Consultation Paper 2026

To the Department of Home Affairs,

I am writing on behalf of **Faithful Drone Services**, a CASA-certified commercial drone operator (██████████) based in South East Queensland. My business provides critical services including infrastructure inspections, construction monitoring, and high-precision mapping for the private and public sectors.

We support the Australian Government's goal of strengthening drone security. However, it is essential that the resulting framework remains **proportionate** and does not create an undue administrative or operational burden on professional, law-abiding operators who already function under strict safety and regulatory oversight.

1. Proactive Management of Drone Threats

- **Operational Integrity:** As a ReOC holder, our operations are already conducted under a vetted Safety Management System. We suggest that security frameworks distinguish between **anonymous, unregistered recreational users** and **licensed commercial entities**. Commercial operators are already "conspicuous" by virtue of our certification and public liability requirements.
- **Sector-Specific Risks:** We agree with the focus on higher-risk places such as critical infrastructure. Our work in asset inspection shows that professional drones are often the *solution* for monitoring these sites securely, rather than being the threat.

2. Enhanced Identification and Tracking (Conspicuity)

- **Remote ID & Privacy:** While we support Remote ID technology for security, the implementation must be **privacy-conscious**. For commercial operators, broadcasting real-time data should be managed so that sensitive client project locations or proprietary flight paths are not accessible to the general public, only to relevant law enforcement agencies.
- **Harmonization:** Any new identification requirements should be harmonized with existing **CASA Remote ID** standards to avoid the need for double-fitting hardware, which would be a significant financial burden on small-to-medium enterprises (SMEs).

3. Counter-Drone (C-UAS) Capabilities

- **Protection of Lawful Users:** In areas where counter-drone systems are deployed (e.g., ports or major events), there must be a **"Safe List" or "De-confliction" process** for ReOC holders. Lawful commercial operations, such as inspecting a bridge or filming an event, should not be disrupted or accidentally "jammed" by automated security systems.

- **Inter-Agency Communication:** We advocate for a streamlined process where local police or security agencies have real-time visibility of authorized commercial flights (perhaps via AVCRM or similar integrated platforms) to prevent unnecessary security responses.

4. Balanced Enforcement & Public Awareness

- **Targeted Enforcement:** Enforcement should focus on deterring willful misuse and non-compliant operators. We support increased penalties for those operating without an RePL or ReOC in restricted security zones.
- **Education:** We recommend a government-led awareness campaign that highlights the **benefits** of professional drone use. Public security perception should not negatively impact the social license for businesses like ours to provide safe, aerial data services.

Conclusion

Faithful Drone Services remains committed to the highest standards of security and safety. We urge the Department to ensure that future policies support "**Security-Informed Innovation**"—where professional operators are seen as partners in national security rather than a risk to be mitigated.

Sincerely,

[Redacted Signature]

Chief Remote Pilot | Faithful Drone Services

[Redacted Address Line]

Email : FaithfulDroneServices@gmail.com

Webpage : <https://FaithfulDrone.FaithfulDental.com.au>

