Submission: Consultation on Proposed Approaches to Australia's Drone Security

1. Submitter Information

Adi Mogilevsky
Managing Director, Synctegral Pty Ltd

- Certified **ReOC (Remote Operator Certificate) holder**
- Technology practitioner specialising in IoT, SAP backend integration, and real-time data streaming
- **Third place (Bronze) winner – SAP Global TechEd Demo Jam 2023** for breakthrough live drone data streaming into enterprise systems

2. Executive Summary

This submission supports the initiative led by the Department of Home Affairs to strengthen drone security while maintaining innovation.

It introduces two key recommendations:

1. **Secure Drone Data Pipeline Framework** – addressing cybersecurity risks in drone-to-backend data streaming
2. **Establishment of a 24/7 National Drone Security Monitoring and Response Capability** – integrating government and industry expertise

These recommendations reflect practical operational and technical experience and aim to close critical gaps in the current approach.

3. Practical Experience and Observations

Through development of a universal IoT integration platform, Synctegral has demonstrated:

- Real-time streaming of drone telemetry and sensor data
- Integration into enterprise systems (e.g. SAP S/4HANA, analytics platforms)
- Automated incident detection and response workflows

This work confirms:

Drone security risks extend beyond the physical drone into the digital ecosystem and response capability

4. Key Risk Areas Identified

4.1 Data Streaming and Backend Exposure

- Unsecured IoT protocols (MQTT, APIs)
- Lack of authentication between drone and backend
- Potential for data spoofing or manipulation

4.2 Fragmented Incident Response

- No centralised real-time visibility across jurisdictions
- Limited integration between:
    - Government agencies
    - Critical infrastructure operators
    - Technical SMEs and solution providers

5. Recommendations

5.1 Secure Drone Data Pipeline Standard

Introduce national requirements for:

- End-to-end encryption (drone → backend)
- Mutual authentication (device + system identity)
- Secure API gateways
- Data validation and anti-spoofing controls

5.2 Drone Digital Identity Framework

- Unique cryptographic identity per drone
- Binding between:
    - Drone hardware
    - Operator (ReOC/RePL)
    - Backend systems

5.3 Certification of Drone & IoT Integration Platforms

- Accreditation scheme for middleware providers
- Compliance requirements for:
    - Protocol handling
    - Data security
    - System interoperability

5.4 Establishment of a 24/7 National Drone Security Monitoring and Response Centre

This is a **critical recommendation**.

Purpose

Create a **centralised, continuously operating "Situation Room"** to:

- Monitor drone-related security incidents in real time
- Correlate physical drone activity with cyber/data anomalies
- Coordinate rapid response across jurisdictions

Core Capabilities

1. Real-Time Monitoring

- Aggregation of:
  - Drone Remote ID data
  - Airspace monitoring systems
  - Critical infrastructure alerts
  - Backend data anomaly signals

2. Incident Correlation

- Link:
  - Physical drone presence
  - Data stream anomalies
  - Cybersecurity alerts

3. Coordinated Response

- Interface with:
  - Law enforcement
  - Emergency services
  - Critical infrastructure operators

4. SME Integration Framework (Key Differentiator)

A unique and high-impact addition:

Establish a **registered panel of vetted SMEs (Subject Matter Experts)** available to support incident response in real time.

These may include:

- Drone operators (ReOC holders)
- IoT and cybersecurity specialists
- Counter-drone technology providers
- Systems integrators

How it would work:

- SMEs are pre-registered, vetted, and categorised by expertise
- The Situation Room can:
  - Rapidly engage SMEs during incidents
  - Provide technical escalation support
  - Assist in forensic analysis and recovery

5. Industry-Government Collaboration Model

- Operate similarly to a **fusion centre**:
  - Government-led
  - Industry-supported
- Integrate with existing frameworks (e.g. critical infrastructure protection mechanisms)

6. Benefits

- Faster incident detection and response
- Reduced fragmentation across agencies
- Real-time access to specialised expertise
- Stronger national resilience against both physical and cyber drone threats

5.5 Expand Counter-Drone Framework to Data Layer

- Detect spoofed or manipulated drone data
- Enable shutdown of compromised integrations
- Monitor anomalous behaviour patterns

5.6 Risk-Based Regulation

- Focus stricter controls on:
  - Critical infrastructure
  - High-risk operations
- Maintain flexibility for:
  - Commercial innovation
  - SMEs and startups

6. Use Case Example

Drone streams real-time radiation data into enterprise systems:

- Triggers alerts and incident workflows
- Visualised live in analytics platforms

Risk:

- False or manipulated data → incorrect emergency response
- Missed anomaly → public safety failure

7. Strategic Impact

These proposals position Australia to:

- Lead globally in **secure drone ecosystem design**
- Integrate **cybersecurity and aviation policy**
- Build a **resilient, collaborative response capability**

8. Conclusion

Drone security must evolve from:

"Managing drones in airspace" → "Securing the entire drone ecosystem (device, data, and response"

In addition of:

- A **secure data pipeline framework**, and
- A **24/7 monitoring and SME-enabled response centre**

will significantly strengthen Australia's national capability.

9. Final Recommendations (Summary)

- Establish a **Secure Drone Data Pipeline Standard**
- Implement **Drone Digital Identity Framework**
- Certify **IoT/Drone Integration Platforms**
- Create a **24/7 National Drone Security Monitoring & Response Centre**
- Enable **SME participation in incident response**
- Extend counter-drone to **cyber/data threats**
- Apply **risk-based regulatory approach**