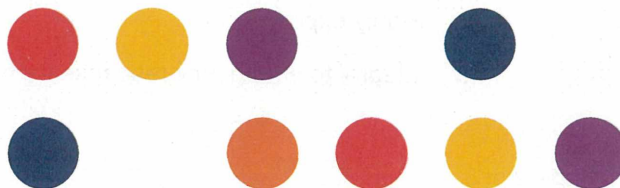


Drone Security

Department of Home Affairs

25 May 2026



Submission

TPG Telecom welcomes the opportunity to provide a submission in response to the Drone Security Public Consultation Paper April 2026.

About TPG Telecom

TPG Telecom Limited is a leading challenger full-service telecommunications provider and own and operate a nationwide mobile network that is connecting Australia for the better. We operate leading mobile and internet brands including Vodafone, TPG, iiNet, Lebara and felix mobile.

Executive Summary

TPG Telecom supports the review of drone security and changes that would provide improved security for critical infrastructure and in particular our telecommunications infrastructure which can be impacted not just by the physical presence of drones but also by radio frequencies they use and by solutions that jam their signals curtailing their ability to operate. The paper deals with drones with a focus on radio operated drones, but drones are now smarter and require no signal to operate or may use fibre optic cable for instructions and this requires more thought to ensure improved security of drone operation. Key points are:

- Telecommunications networks are critical infrastructure under the SOCI Act, underpinning:
 - Triple Zero (000) emergency calling
 - Public warning systems (including cell broadcast emergency alerts)
 - Continuity of communications during natural disasters and major incidents
- The distributed and accessible nature of mobile network infrastructure (towers, antennas, backhaul) creates a unique exposure to drone-related risks, including:
 - Physical damage to assets
 - Radiofrequency (RF) interference
 - Service disruption with direct public safety consequences
- The proposed drone framework should explicitly recognise telecommunications infrastructure as:
 - Safety-critical
 - Highly exposed
 - Integral to emergency response frameworks

TPG Telecom recommend the framework:

- Introduce risk-based exclusion zones around telecommunications infrastructure
- Enable licensed and authorised drone use for telecommunications operations
- Establish minimum technical and RF compliance standards
- Implement strict safeguards on RF jamming, given risks to emergency communications

Failure to address these issues risks undermining emergency calling, delaying public warnings, and weakening national resilience during emergencies.

Our specific responses to questions as follows:

What are the key risks posed by drones?

TPG Telecom believes that

- Telecommunications infrastructure faces specific risks due to:
 - Highly distributed network footprint (towers, rooftop sites, backhaul links)
 - Limited physical protection in many locations
- Key risks include:
 - Physical impact damage to antennas, towers, and cables
 - Service outages, which may:
 - Disrupt Triple Zero calls
 - Prevent delivery of cell broadcast (AusAlert) and SMS (Emergency Alert) emergency alerts
 - Cascading network impacts, particularly in:
 - Regional or single-site coverage areas
 - Electromagnetic interference (EMI) affecting:
 - Telecommunications equipment
 - Drone control systems
- These risks have immediate public safety implications, particularly during emergencies where communications are critical.

What infrastructure should be prioritised or protected?

TPG Telecom holds a strong view that telecommunications infrastructure protections should be explicitly included, such as:

- Mobile base stations (towers and rooftop installations)
- Antenna systems
- Transmission and backhaul infrastructure (including microwave links), satellite ground stations, etc.
- Rationale:
 - Supports Emergency Call Service (ECS) obligations
 - Enables cell based (AusAlert) and SMS (Emergency Alert) emergency warning systems
 - Critical for emergency services coordination and public communication
- Telecommunications networks should be recognised as:
 - Critical infrastructure under SOCI
 - In some cases, part of a System of National Significance

Do you support exclusion zones or airspace restrictions?

Yes – TPG Telecom strongly support risk-based exclusion and restricted zones

- Recommended measures:
 - Establish minimum separation distances from:
 - Mobile towers
 - Antennas
 - Backhaul links
 - Satellite ground stations; and
 - Any other telecommunications infrastructure
 - Integrate telecommunications infrastructure into:
 - Geofencing systems

- Restricted airspace frameworks
- Risk-based approach should consider:
 - Sites critical to emergency coverage
 - High-density population areas
- Justification:
 - Protects against:
 - Physical damage
 - RF interference
 - Disruptions to Triple Zero and both cell based (AusAlert) and SMS (Emergency Alert) emergency alert systems

How should legitimate drone use be supported?

Yes. TPG Telecom, our contractors and other telecommunications operators currently use and rely upon drones for:

- Infrastructure inspections
- Fault detection
- Post-disaster response and recovery
- These uses support:
 - Rapid restoration of services, including emergency communications
 - Compliance with network reliability and outage obligations
- Recommended approach:
 - Introduce licensing/accreditation framework for:
 - Carriers and carriage service providers
 - Approved contractors
 - Permit:
 - Access to restricted zones for authorised purposes
 - Expedited approvals during emergencies

- Regulatory alignment:
 - CASA aviation rules
 - Telecommunications obligations (including ECS continuity)
-

What technical or operational requirements should apply?

TPG Telecom supports minimum technical standards for drones operating near telecommunications infrastructure

- Proposed requirements:
 - RF resilience and shielding capability
 - Ability to safely operate in high electromagnetic environments
 - Fail-safe functions:
 - Return-to-home
 - Controlled landing
 - Consider certification for:
 - Drones authorised to operate within proximity thresholds
 - Objective:
 - Reduce risk of:
 - Loss-of-control incidents
 - Interference with telecommunications networks
 - Disruption to emergency communications and alerting systems
-

Views on counter-drone measures (e.g. jamming)

TPG Telecom has significant concerns regarding RF jamming technologies and their potential for unintended consequences.

- Risks include:
 - Harmful interference with licensed telecommunications spectrum
 - Disruption to:

- Triple Zero calls
 - Cell broadcast emergency alerts
 - General public communications
 - Recommended controls:
 - Maintain and possibly strengthen the existing controls on the use of jammers and limit use to authorised government entities and their contracted providers only
 - Require:
 - Spectrum impact assessments
 - Ongoing coordination with telecommunications operators
 - Important limitations:
 - Jamming ineffective against:
 - Autonomous drones
 - Fibre optic tethered drones
 - Recommend a multi-layered approach, not reliance on jamming alone
-

Are there gaps or additional considerations?

TPG Telecom view is that there is scope for the framework to more explicitly address:

- Impacts on telecommunications-supported public safety services (e.g. emergency alerts solutions and temporary disaster roaming)
- Interdependencies with:
 - Emergency call services (000)
 - National emergency warning systems (i.e. AusAlert and Emergency Alert)
- Current gap:
 - There is limited consideration of non-RF controlled drones
- Recommend:
 - Alignment with:
 - Security of Critical Infrastructure framework

Public

- Broader telecommunications resilience obligations
- Inclusion of telecommunications sector in:
 - Ongoing policy development
 - Operational coordination mechanisms

Additional comments

Telecommunications infrastructure is foundational to public safety and emergency response

- Any disruption can have immediate and severe consequences, particularly during natural disasters
- The drone security framework should:
 - Explicitly recognise telecommunications as critical safety infrastructure
 - Ensure alignment with existing:
 - Regulatory obligations (e.g. regulation that applies to use of signal jamming equipment)
 - Emergency management frameworks
- A balanced approach is required to:
 - Protect infrastructure
 - Enable innovation
 - Maintain resilient, continuous communications for the Australian community.