



AFP

AUSTRALIAN FEDERAL POLICE



Australian Communications and Media Authority

Consultation into arrangements for jamming devices and radiocommunications device exemptions

20 July 2020

Submission by the
Australian Federal Police

Introduction.....	3
Radiocommunications prohibition and exemption framework.....	3
Exemption regime	3
Impracticality of the current framework.....	3
Risk to AFP methodologies becoming public	4
.....	4
Suggested proposal to amend the Radiocommunications Act	4
Prohibition regime	5
Terminology consistency.....	6
'Police forces' vs 'Law enforcement'.....	6
Definition of 'Drones'	6
Conclusion.....	6

Introduction

1. The Australian Federal Police (AFP) welcomes the opportunity to make this submission to the Australian Communications and Media Authority (ACMA) as part of consultations into the radiocommunications prohibition and exemption framework, and arrangements for law enforcement use of drone jamming devices, under the *Radiocommunications Act 1992* (the Act).
2. Drones are increasingly being used for malicious purposes, such as weaponised drones being used to deliver explosives, firearms or chemical dispersion attacks. To coordinate law enforcement's response to the malicious or terrorist use of drones, the Australia New Zealand Counter-Terrorism Committee (ANZCTC) has established a Counter-Remotely Piloted Aircraft System (C-RPAS) working group.
3. The AFP supports ACMA's proposed *Radiocommunications (Police Forces – Disruption of Unmanned Aircraft) Determination* (proposed police exemption) to exempt police with respect to the possession, operation and supply of drone jamming devices. This proposal would have the practical effect of authorising police to deploy drone jamming devices to protect critical infrastructure, at major events and for other policing operations, without needing to seek individual exemptions.
4. In addition to the proposed police exemption, the AFP suggests a general exemption for the AFP, similar to the partial exemption under section 24 of the Act for intelligence agencies, noting that the AFP is part of the National Intelligence Community (as defined under the Office of National Intelligence Act 2018), providing criminal and other intelligence capabilities across all operational functions and crime types. This would be beneficial to enhance policing capabilities to use other unlicensed or prohibited radiocommunication devices to combat crime.
5. In relation to the prohibition regime of the framework, the AFP strongly supports consistency in legislation and technologically neutral provisions to accommodate advances in technology, except where specificity is appropriate.

Radiocommunications prohibition and exemption framework

Exemption regime

6. The current radiocommunications exemptions framework does not adequately meet AFP needs. Under the current framework the stakeholder engagement and consultation process:
 - creates impracticalities in a law enforcement environment
 - affords undue public exposure of sensitive capabilities that may be used by the AFP and other law enforcement
 - [REDACTED]

Impracticality of the current framework

7. Section 46 of the Act requires that radiocommunications devices be licensed, and section 47 of the Act contains offences for unlicensed possession. Both these provisions allow a defence with 'reasonable excuse'. Further, section 27 allows law enforcement to apply for a general or specific exemption.
8. While the AFP currently has a significant number of radiocommunications licenses, obtaining a license to use radiocommunication devices, is at times, impractical.
9. Radiocommunications device licenses carry different conditions that restrict the use of devices to parts of the spectrum, particular places, periods of time or levels of radio

emissions. This is not viable for all policing operations should they require use of a device outside of the license condition, on an ad hoc or time-critical basis.

10. As a result, the AFP is currently required to seek event specific exemptions under section 27 to use prohibited or unlicensed devices, which includes the use of radio communications jamming devices.
11. The current framework lacks the agility required for police to responsively access and utilise some technologies to mitigate national security and public safety issues. Further, the law enforcement exemption process under section 27(2) is a protracted process which may delay or prevent time-critical investigative activities.
12. Since exemptions are at the discretion of the ACMA, they are not guaranteed and can therefore interfere with time-critical police operational activities, should such exemptions not be approved, or not be approved in time, with a time.

Risk to AFP methodologies becoming public

13. There are also concerns that, through the exemption process, AFP methodologies and capabilities may be disclosed. Given that exemption determinations are considered legislative instruments for the purposes of the *Legislative Instruments Act 2003* (Cth), any approved exemption is published and publically accessible on the Federal Register of Legislation website, along with the supporting explanatory statement. Disclosure can alert criminal groups to AFP methodologies, capabilities and vulnerabilities.

14. [REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Suggested proposal to amend the Radiocommunications Act

18. The ACMA proposed *Radiocommunications (Police Forces – Disruption of Unmanned Aircraft)* exemption is **strongly supported** by the AFP, noting it proposes a general exemption under section 27(2) of the Act for police to use counter drone capabilities and test and maintain drone jamming devices. These proposed provisions would allow the AFP to operate drone jamming devices in the interest of public safety, [REDACTED]
[REDACTED] As noted, seeking individual exemptions is operationally impractical and risks disclosing police methodologies.
19. In addition, the proposed 2020 determination goes further than the *Radiocommunications (Unmanned Aircraft and Unmanned Aircraft Systems) Exemption Determination 2019* as it expands the exemption to state and territory police jurisdictions, as well as their relevant

contractors. This affords states and territories a level of self-sufficiency to counter drone related security threats within their own jurisdiction.

20. As a member of the ANZCTC C-RPAS working group, the AFP supports the proposed exemption determination as it will support police use of technology to defend against the national security and public safety threats posed by drones.
21. The AFP also supports the wide range of 'relevant frequency bands' identified in the 2020 determination as specified in the *Radiocommunications (Low Interference Potential Devices) Class Licence 2015* legislative instrument.
22. To better support the undertaking of its role and functions, the AFP seeks inclusion as a listed agency for a statutory exemption in sections 24(1) and 24(2) of the Act, in line with the Defence Force, Department of Defence, the Australian Secret Intelligence Service (ASIS), the Australian Security Intelligence Organisation (ASIO), and the Australian Signals Directorate.
23. Inclusion of the AFP in section 24(2) would provide the AFP with the required flexibility to deploy technologies that may be prohibited or otherwise unlicensed under the Act in order to exercise its functions as set out in section 8 of the *Australian Federal Police Act 1979*. This amendment would also recognise:
 - the AFP is an integral agency to Australia's national security
 - the AFP's remit includes the investigation of sensitive and unique crime types such as terrorism and foreign interference
 - the AFP's good record of regulatory compliance with respect to the Act, and considerable strategic and operational experience in management of risks associated with the deployment of prohibited devices under an exemption determination.

Prohibition regime

24. Given developments in the capabilities of devices and their accessibility, the current prohibitions are no longer fit-for-purpose and hinder effective policing activities.
25. Section 190 of the Act provides legislative authority to the ACMA to make declarations that the *operation or supply or possession for the purpose of operation or supply of a specified device* is prohibited.
26. Under the Act, the ACMA has made two prohibition declarations, prohibiting mobile phone jamming devices and GPS jamming devices. The only exemptions to these prohibitions are for:
 - electronic counter measures for bomb disposal activities, visiting forces and suppliers;
 - the New South Wales Crime Commission for using, operating, possessing or supplying a surveillance device;
 - a blanket exemption by Defence personnel to GPS jamming devices; and
 - The AFP using defined counter-drone capability.
27. The AFP notes the prohibitions on mobile phone jamming devices was broadened in 2011 to not restrict mobile telecommunications to specified frequency bands.¹ However, the AFP does appreciate ACMA's consultations paper position that these prohibitions remain static.
28. The AFP strongly supports the use of technologically neutral language in legislation, unless specificity is required. As such, the AFP supports amendments to the prohibitions to ensure they are technologically neutral to accommodate advances in technology. However, the AFP

¹ see the *Radiocommunications (Prohibition of PMTS Jamming Devices) Declaration 2011*

would not necessarily support other frequencies or technologies being incorporated into the collective PMTS category.

Terminology consistency

29. The AFP notes there are a number of terminology inconsistencies between the proposed 2020 exemption determination and ACMA's consultation paper on *Radiocommunications exemptions for Law Enforcement use of Drone Jamming Devices*.

'Police forces' vs 'Law enforcement'

30. The exemption determination limits the use of drone jamming devices to *police forces*. However, the title of the consultation paper provides for '*law enforcement* use of drone jamming devices'. The AFP notes that the term 'law enforcement' can be applied broadly to include not just police but a range of Commonwealth, State and Territory entities that enforce legislation (for example state and territory crime commissions and prosecutions services). As such, the AFP suggests it be clarified that the exemption will extend only to 'police forces' in accordance with the proposed police exemption determination.

Definition of 'Drones'

31. The AFP notes that the consultation paper advises that the term 'drone' includes 'unmanned aircraft' (UA), 'unmanned aircraft systems' (UAS) and 'remotely piloted aircraft systems' (RPAS). However, the proposed exemption determination only refers to UA and UAS, excluding RPAS.

32. The *Civil Aviation Safety Regulations 1998* provide legislative definitions for Remotely Piloted Aircraft (RPA) and RPAS. Since 2016, the Civil Aviation Safety Authority (CASA) has adopted these as the official terms, which have replaced the terms UAS and UA.

33. For consistency and clarity, the AFP recommends the determination use the term 'RPAS', to negate ambiguity and ensure the determination aligns with official terminology. Should there be a requirement that the determination use the term UAS, the AFP recommends that the definition of be amended to expressly reference RPAS, noting it is an interchangeable term. This will provide clear guidance as to what types of drones are captured by the determination and recognises official terminology as per the *Civil Aviation Safety Regulations 1998*, as used by CASA.

Conclusion

34. The AFP appreciates the opportunity to make this submission to the ACMA in relation to the consultation papers on the arrangements for jamming devices and radiocommunications device exemptions. The AFP supports the proposed 2020 exemption determination to exempt police from offences related to drone jamming devices, however suggests that the Act be amended to include the AFP as a listed agency under section 24(1) and 24 (2) the Act. This would provide the AFP with the required flexibility to deploy technologies that may be prohibited or otherwise unlicensed under the Act, in order to support policing capabilities in an ever evolving technology environment.