EXPLANATORY STATEMENT

Issued by authority of the Attorney-General

Telecommunications (Interception and Access) Act 1979

Telecommunications (Interception and Access) (Communications Access Coordinator) Instrument 2024

1 The instrument is made under subsection 6R(2) of the *Telecommunications (Interception and Access) Act 1979* (the TIA Act).

2 The instrument commences on the day after registration on the Federal Register of Legislation, and is a legislative instrument for purposes of the *Legislation Act 2003* (the Legislation Act).

Purpose

3 The TIA Act establishes the position of *Communications Access Coordinator* (CAC) as the primary point of liaison for interception agencies and telecommunications carriers and carriage service providers in relation to telecommunications interception and data retention issues.

4 Under section 6R of the TIA Act, a CAC is the Secretary of the Attorney-General's Department or a person or body specified by the Attorney-General in a legislative instrument under that section. Under subsection 6R(2), a legislative instrument may specify one or more persons or bodies, or one or more classes of persons or bodies, as a CAC. Under subsection 6R(2A), specification of a person or class of persons is limited to APS employees, or a class consisting wholly of APS employees, in the Attorney-General's Department.

5 The instrument specifies persons who hold or perform the duties of certain positions in the High Tech Crime Branch of the National Security and Criminal Justice Group in the Attorney-General's Department, or are SES Band 2 or 3 with responsibility for the High Tech Crime Branch, as a CAC.

6 The instrument also limits the specification in relation to certain sections of the TIA Act and the *Telecommunications Act 1997* (Telecommunications Act). These limitations respond to concerns raised by the Standing Committee for the Scrutiny of Delegated Legislation about the specifications in the 2022 instrument made under previous subsection 6R(2).

Consultation

7 No consultation was undertaken prior to making the instrument, as it makes technical changes that do not affect the powers or functions of the CAC.

Details of the instrument

8 Section 1 sets out the name of the instrument.

9 Section 2 provides for the commencement of the instrument on the day after registration.

10 Section 3 notes the instrument is made under subsection 6R(2) of the TIA Act.

11 Section 4 defines words and terms used in the instrument.

12 Section 5 of the instrument specifies persons who hold or perform the duties of the listed positions in the High Tech Crime Branch of the National Security and Criminal Justice Group, or are SES Band 2 or Band 3 with responsibility for the High Tech Crime Branch, in the Attorney-General's Department, to be a CAC for the purposes of paragraph (b) of the definition of *Communications Access Coordinator* in subsection 6R(1) of the TIA Act.

13 This section does not affect the ability of the Secretary to exercise these powers or functions as a CAC under paragraph (a) of the definition of *Communications Access Coordinator* in subsection 6R(1) of the TIA Act.

Powers and functions that may only be exercised by Senior Executive Service (SES) officers, or the Secretary

14 Subsections 5(1), (4) and (6) specify certain powers or functions under the TIA Act and the *Telecommunications Act 1997* (the Telecommunications Act) that are to be limited to the SES Band 1, 2 or 3 level.

15 For the TIA Act, the specified functions that may only be exercised by officers at the SES level are:

- Section 183 – which allows a CAC to determine requirements, through a legislative instrument, for the content of authorisations given by agencies authorising providers to disclose telecommunications data, and requires the CAC to consult the Australian Communications and Media Authority (ACMA) and the Information Commissioner in relation to matters that relate to privacy functions before making a determination

- Section 187B – which allows a CAC to declare that mandatory data retention regime (MDRR) obligations under section 187A apply in relation to a service, even if they otherwise do not apply, and requires the CAC to give this declaration to the Minister

- Section 187F, subsection187G(6) and section 187J – which allow a CAC to approve and amend a data retention implementation plan

- Subsection 187K(1), paragraph 187K(5)(b), and subsections 187K(6), 187K(7) and 187K(8) – which allow a CAC to exempt or vary a service provider's data retention obligations

- Subsection 188(4) – which allows a CAC to refer a disagreement about the location of a delivery point to the ACMA for a determination

- Section 202B – which allows a CAC to prevent a provider from making a proposed business change that would have a material adverse effect on compliance with the TIA Act or section 313 of the Telecommunications Act, and

- Subsection 203(1) – which allows a CAC to specify delivery capability parameters for lawfully intercepted information after consulting with ACMA.

16 For the Telecommunications Act, the specified function that may only be exercised by officers at the SES level is:

- Section 56A – which allows a CAC to give notice to ACMA to not grant a carrier licence (for a period of 3 months that can be renewed for up to 12 months or revoked at any time by notice to ACMA).

17 Subsection 5(6) specifies that functions under the *Interception Capability Plan Determination 2024* and the *Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination 2017* are to be exercised only at the SES level. Under the *Interception Capability Plan Determination 2024* a CAC can request additional information relating to how the carrier or nominated carrier service provider will uphold its legal obligations to provide interception capabilities. The ACMA may make a determination under section 99 of the Telecommunications Act setting out rules for the supply of specified services. The *Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination 2017* is made under this section, and requires ACMA to consult the CAC on alternative ID check compliance plans.

Powers and functions that may be exercised by Executive Level or SES officers, or the Secretary

18 Subsection 5(2) specifies certain powers or functions under the TIA Act that may be performed by Executive Level 1 or Executive Level 2 officers in addition to SES officers. These are:

- Subsections 187G(2) and (4) – these provisions apply where an agency has requested that a service provider amend a data retention implementation plan, and require the CAC to:
    - convey they agency's request to the service provider and,
    - if the service provider does not agree to make the requested amendment, to refer the request and the service provider's response to the ACMA to determine whether amendments are required, and
- Sections 192, 196, 197 and 198 – which require that a CAC be given an interception capability plan by each carrier/nominated carriage service provider and allow a CAC to approve those plans, request additional information or amendments, and grant certain exemptions.

Powers and functions that may be exercised by Australian Public Service, Executive Level or SES officers, or the Secretary

19 Subsections 5(3) and (5) specify certain powers or functions under the TIA Act and the Telecommunications Act which may be performed by APS Level 1 to 6 officers, in addition to Executive Level and SES officers.

20 For the TIA Act, the specified functions that may be exercised by officers at APS Level and above are:

- sections 187G(1) – which requires the CAC to give a copy of applications for data retention implementation plans to enforcement agencies and security authorities to review
- Paragraph 187K(5)(a) – which requires a CAC to give a copy of applications for exemption or variation to mandatory data retention regime obligations to ACMA, as well as interested law enforcement agencies and security authorities
- Section 187L – which deals with the confidentiality and disclosure of applications for the approval of data retention implementation plans and exemptions and variations to service providers' data retention obligations
- Subsection 188(2) – which provides that a CAC may notify a carrier if an interception agency disagrees with the location of a delivery point

- Paragraph 188(9)(c) – which provides that a CAC may convey requests from agencies to carriers to nominate alternative delivery point locations

- Section 202 – which deals with the confidentiality and disclosure of interception capability plans

- Section 202C – which allows a CAC to notify agencies that are likely to be interested about proposed changes to a service provider's service or system, the implementation of which may affect the provider's ability to comply with its obligations under the Act or section 313 of the Telecommunications Act and requires the CAC to treat the proposed change as confidential.

- Subsection 203(3) – which requires a CAC to consult ACMA before making a determination under subsection 203(1).

21 For the Telecommunications Act, the specified functions that may be exercised by officers at the APS Level and above are:

- Section 53A – requires receipt by a CAC of a carrier application for the purposes of sections 56A and 59 of the Telecommunications Act; for the avoidance of doubt, the specification clarifies which officers in the department this information can be provided to discharge the requirement in section 53A

- Section 317ZF – which deals with the confidentiality and disclosure of certain information concerning technical assistance requests, technical assistance notices and technical capability notices.

Powers and functions that may only be exercised by the Secretary

22 The following powers and functions are not included in the instrument and will be exercisable only by the Secretary of the Attorney-General's Department:

- clause 126 of Schedule 1 of the TIA Act – which enables a CAC to apply to the Federal Court of Australia or the Federal Circuit and Family Court of Australia for the enforcement of civil penalty provisions relating to the international production order framework, and

- sections 317ZC, 317ZD and 317ZE of the Telecommunications Act – which enable a CAC to apply to the Federal Court of Australia or the Federal Circuit and Family Court of Australia (Division 2) for the enforcement of civil penalty provisions, or for enforceable undertakings or injunctions, relating to compliance with a technical assistance notice or a technical capability notice under section 317ZB of the Telecommunications Act.

Specification of particular positions

23 In assigning CAC-related functions to particular classification levels, the Attorney-General's Department has had regard to the Australian Public Service Commission's APS Work Level standards and Integrated Leadership System. In addition, sections 25 to 29 of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) set out the general duties that apply to officials and require all officials to meet high standards of governance, performance and accountability.

24 The framework for the assessment of interception capability plans and interception capability exemption requests (sections 196, 197 and 198) involves high-volume, time-sensitive decision-making undertaken in close consultation with interception agencies. For example, from 1 May to 30 September

2024, there were 248 decisions on ICPs and 20 decisions on ICEs. It is appropriate for these decisions to be taken by Executive Level officers, noting the training and technical assistance arrangements in place to support that decision-making, as set out below. Similarly, decisions under section 192 to exempt carriage service providers from their interception obligations should be taken by the same decision-maker who considers ICPs, placing decisions in the same context.

25 The framework for the management of agency requests for amendments to data retention implementation plans, including disagreements about such requests, under subsections 187G(2) and (4) does not involve discretionary decision-making by a CAC—the framework requires that agency requests be conveyed to the relevant service provider, and that any disagreement between the relevant agency and service provider be referred to the ACMA for resolution. Authorising Executive Level officers to perform these functions will facilitate the expeditious administration of this framework, while ensuring that senior and experienced officers have visibility of—and the opportunity to engage on, where appropriate—disagreements between agencies and service providers.

26 The receipt and despatch of CAC correspondence to stakeholder agencies, for example as required in subsection 187G(1) and paragraph 187K(5)(a), is a high volume and routine function that is appropriately undertaken by officers at APS levels.

27 It is appropriate that confidentiality requirements associated with CAC functions (for example, sections 187L and 202C of the TIA Act) apply to all officers undertaking those functions, including at APS level, and that agencies and the ACMA be permitted to provide information relevant to CAC functions to those officers.

28 More sensitive or complex decisions are appropriately reserved for SES decision-makers to ensure decisions are subject to additional and appropriate oversight. Examples of such decisions include exempting or varying the obligations imposed on service providers in relation to the mandatory data retention scheme (section 187K(1) of the TIA Act) or issuing a notice (under section 56A of the Telecommunications Act) to ACMA that it may not issue a carrier licence.

29 For all CAC decisions, the Attorney-General's Department has in place systems and processes to ensure CACs are appropriately trained and make decisions commensurate with their classification level.

30 The role of a CAC is supported by significant on-the-job training, mentoring and policy guidance, ensuring all CACs are appropriately qualified to perform the functions and make the decisions assigned to their particular classification level. The Attorney-General's Department also has guides and standard operating procedures in place detailing the processes for making CAC decisions.

31 In addition, the Attorney-General's Department consults closely with law enforcement and national security agencies on decisions requiring technical telecommunications or investigations expertise, so that CACs are appropriately informed of relevant technical issues and the needs of the law enforcement and national security agencies.

Parliamentary scrutiny

32 The instrument is subject to disallowance under section 42 of the Legislation Act. A Statement of Compatibility with Human Rights has been prepared in relation to the instrument, and finds that the instrument does not raise any human rights issues. The Statement is included at **Attachment A** to this explanatory statement.

33 The instrument was made by the Attorney-General in accordance with subsection 6R(2) of the TIA Act.

Attachment A

Statement of Compatibility with Human Rights

Prepared in accordance with Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011

Telecommunications (Interception and Access) (Communications Access Coordinator) Instrument 2024

This disallowable legislative instrument is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.

Overview

The *Telecommunications (Interception and Access) (Communications Access Coordinator) Instrument 2024* (the instrument) is made under subsection 6R(2) of the *Telecommunications (Interception and Access) Act 1979* (the TIA Act).

Under section 6R of the TIA Act, the Communications Access Coordinator (CAC) is the Secretary of the Attorney-General's Department or a person or body specified by the Attorney General in a legislative instrument under that section. Under subsection 6R(2), a legislative instrument may specify one or more persons or bodies, or one or more classes of persons or bodies as a CAC. The specification of a person or class of persons is limited to APS employees, or a class consisting wholly of APS employees, in the Attorney-General's Department.

This instrument defines as a CAC certain persons who hold or perform the duties of the listed positions in the High Tech Crime Branch of the National Security and Criminal Justice Group, or who are SES Band 2 or 3 officers with responsibility for the High Tech Crime Branch, in the Attorney General's Department.

The instrument also limits the specification in relation to certain sections of the TIA Act and the Telecommunications Act. These limitations address concerns raised by the Standing Committee for the Scrutiny of Delegated Legislation in Monitor 8 of 2022 about the delegations in the 2022 instrument made under previous subsection 6R(2).

The instrument is technical in nature, and does not affect the overall powers or functions of a CAC, which are governed by the TIA Act and the Telecommunications Act.

Human rights implications

This instrument is a specification instrument that allows high volume and routine functions of the CAC to be undertaken by Australian Public Service or Executive Level staff, while more complex and sensitive decisions will be required to be made at the SES level, providing additional safeguards and accountability. Allowing other individuals, in addition to the Secretary, to perform particular CAC functions will support the timely and efficient discharge of these functions. This disallowable legislative instrument does not engage any of the applicable rights or freedoms.

Conclusion

This instrument is compatible with human rights as it does not raise any human rights issues.

The Hon Mark Dreyfus KC MP

Attorney-General