Australian Government
Attorney-General's Department

May 2024

Parliamentary Joint Committee on Intelligence and Security

Submission to the Inquiry into the Crimes and Other Legislation Amendment (Omnibus No. 1) Bill 2024 (provisions)

Attorney-General's Department Submission

Introduction

The Attorney-General's Department welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Intelligence and Security's inquiry into the Crimes and Other Legislation (Omnibus No.1) Bill 2024 (the Bill). The purpose of the submission is to provide an overview of the key provisions of the Bill to assist the Committee's inquiry. The submission should be read alongside the Bill and its explanatory materials.

The Bill would make a number of amendments to crime-related provisions in Commonwealth legislation to update, improve and clarify the intended operation of these provisions, including:

- amendments to the *Crimes Act 1914* (Crimes Act), the *Proceeds of Crimes Act 2002* (Proceeds of Crime Act) and the *National Anti-Corruption Commission Act 2022* (NACC Act) to expressly clarify that a warrant may authorise the seizure of digital assets and that an executing officer is able to access a person's digital wallet and transfer its contents as a means of 'seizing' the digital asset (Schedule 1)
- amending the Proceeds of Crime Act to ensure law enforcement authorities' current information-gathering powers and freezing orders apply to digital currency exchanges (Schedule 2)
- amending the Crimes Act to increase the Commonwealth penalty unit amount from $313 to $330, with effect from 1 July 2024 (Schedule 3)
- amending the *Telecommunications (Interception and Access) Act 1979* (TIA Act) and the *Telecommunications Act 1997* (Telecommunications Act) to clarify the functions of the Communications Access Coordinator (CAC) in the Attorney-General's Department, create the position of Communications Security Coordinator (CSC) in the Department of Home Affairs and enable the Attorney-General and the Minister for Home Affairs to authorise officers of their respective departments to perform certain CAC and CSC functions as appropriate (Schedule 4), and

- amend the TIA Act to enhance the ability of specific New South Wales, Victorian, South Australian and Western Australian oversight bodies to receive intercepted information and interception warrant information under the TIA Act (Schedule 5).

The Bill was referred by the Attorney-General to the Committee in line with 110A(11) of the TIA Act, which requires that any amendment to subsection 110A(1) of the TIA Act be referred to the Committee for review. Subsection 110A(1) lists criminal law-enforcement agencies who are able to access stored communications and telecommunications data under the TIA Act. Items 153-158 of Schedule 5 of the Bill will make cosmetic amendments to the TIA Act, specifically to amend subsection 110A(1) to specify the jurisdiction of integrity agencies already included in the TIA Act to aid clarity. The amendments omit 'Crime Commission', 'Independent Commission Against Corruption', 'Law Enforcement Conduct Commission', 'IBAC', 'Crime and Corruption Commission' and 'Corruption and Crime Commission' and substitute with 'Crime Commission (NSW)', 'Independent Commission Against Corruption (NSW)', 'Law Enforcement Conduct Commission (NSW)', 'IBAC (Vic.)', 'Crime and Corruption Commission (Qld)' and 'Corruption and Crime Commission (WA)'. The amendments do not change, or otherwise alter, the existing powers available to these agencies under the TIA Act.

Provisions of the Bill

Schedule 1 – seizing digital assets

This schedule would amend the Crimes Act, the Proceeds of Crime Act and the NACC Act to strengthen the legal framework relating to the seizure of digital assets. Law enforcement agencies have identified an increase in criminals' use of digital assets (including cryptocurrency) to facilitate their offending and as a means to hold and distribute the benefits derived from their offending. Investigations involving digital assets have been associated with a variety of crime types including the purchase of drugs, child exploitation material and firearms through dark web markets; ransomware and cyber related offences; and money laundering and financing of terrorist organisations.

The schedule inserts a new definition of 'digital asset' that is flexible enough to encompass both the terms that are currently used in the crypto-asset industry like coins, stablecoins and tokens, and those that may emerge as the technology evolves. These amendments do not grant additional powers to law enforcement agencies. Instead, they ensure the existing powers available to law enforcement can account for the increasing prevalence of digital assets in law enforcement operations.

The proposed amendments would expressly clarify that a warrant may authorise the seizure of digital assets and that an executing officer is able to access a person's digital wallet and transfer its contents as a means of 'seizing' the digital asset. The amendments would achieve this by inserting a new section in the Crimes Act and the Proceeds of Crime Act that lists ways that digital assets can be seized and clarifies that a warrant may authorise the use of electronic equipment to seize digital assets or access other relevant data.

To ensure that the use of powers is appropriately targeted, the amendments will also clarify the circumstances in which cryptocurrency and other digital assets can be seized in relation to warrants over premises and persons, and establish the appropriate thresholds for the seizure of digital assets. For example, the executing officer needs to reasonably suspect that the seizure of the digital asset is necessary to prevent the digital asset's concealment, loss or destruction or its use in committing an offence. Furthermore, the Bill

provides that safeguards in the existing legislation which govern the time periods law enforcement can retain things moved or seized under warrant will also apply to the digital asset seizure measure.

Schedule 2 – digital currency exchanges

The Proceeds of Crime Act provides law enforcement authorities with broad powers to monitor, freeze, restrain and forfeit proceeds and instruments of crime. These powers currently apply to financial institutions. The amendments would extend the investigative and freezing powers to apply to certain digital currency exchanges.

This schedule would expand the definition of 'financial institution' to include a corporation that provides a digital currency exchange, ensuring the notices and orders provided under the proceeds of crime regime can be extended to a digital currency exchange.

The expansion of the regime to include digital currency exchanges retains existing safeguards, including that:

- freezing orders and monitoring orders are subject to independent oversight, such that the relevant orders must be made by a magistrate after considering whether the legislative requirements for making the order have been met
- the orders only operate for a set period of time and need to be reviewed by a magistrate if they are to be extended, and
- a magistrate would have the power to vary a freezing order to enable a financial institution to allow a withdrawal from the account to meet the reasonable living expenses of the person, dependents of the person, business expenses of the person, or a specified debt incurred in good faith by the person.

Schedule 3 – increase the value of the penalty unit

This schedule would amend the Crimes Act to increase the Commonwealth penalty unit from $313 to $330. The new penalty unit value will only apply to offences which are committed on or after the day the amendments come into force.

Penalty units are used to describe the amount payable for monetary penalties imposed for criminal offences and contraventions of civil provisions in Commonwealth legislation and territory ordinances where penalties are commonly expressed in penalty units, rather than a fixed monetary sum. The penalty unit mechanism allows for the maximum monetary penalty for all offences under Commonwealth law, including territory ordinances, to be automatically adjusted with a single amendment to section 4AA of the Crimes Act, and removes the need for multiple legislative amendments.

Maintaining the value of the penalty unit over time ensures that financial penalties for Commonwealth offences reflect community expectations and continue to remain effective in deterring unlawful behaviour. Offences that attract financial penalties expressed in penalty units include serious drug offences, people smuggling, cybercrime and money laundering.

Fines are the most common sentencing disposition imposed by courts in Commonwealth matters, occurring in 31% of sentencing matters in the 2021–22 financial year.[1] The value of the penalty unit has increased five times by legislative amendment and twice by automatic indexation since it was first instituted in 1992,

[1] Australian Bureau of Statistics (May 2023) Federal Defendants, Australia, abs.gov.au, accessed 23 April, 2024.

increasing from $100 to $313 (currently). These increases represent an increase of 213%, while average incomes have increased by 282% during the same period.[2]

Increasing the value of a penalty unit does not curb the court's existing discretion to impose a penalty that is appropriate with regard to all the circumstances. Rather, increasing the value of a penalty unit increases the maximum penalty that the court can impose as punishment for the most serious offending.

In 2015, the Crimes Act was amended to provide for the automatic Consumer Price Index adjustment of penalty units every three years. The three yearly indexation cycle will continue as usual, with the next indexation increase occurring on 1 July 2026, which is three years from the last automatic indexation.

Schedule 4 – Communications Access Coordinator and Communications Security Coordinator

This schedule would amend the TIA Act and the Telecommunications Act to clarify the functions of the Communications Access Coordinator (CAC) in the Attorney-General's Department and create the position of Communications Security Coordinator (CSC) in the Department of Home Affairs.

The CAC is a specified position within the Attorney-General's Department responsible for liaising between security and law enforcement agencies and the telecommunications industry, to support industry in understanding its interception capability, and data retention and security obligations under the TIA Act. The CAC's statutory roles include approving interception capability plans and considering and approving exemptions from interception capability and data retention obligations. The CAC also has functions relating to the issuing of carrier licences by the Australian Communications and Media Authority (ACMA) under Part 3 of the Telecommunications Act.

Under Part 14 of the Telecommunications Act, the CAC is responsible for responding to notifications from service providers regarding proposed changes to their telecommunications services or systems which may be prejudicial to security. The CAC's functions under Part 14 relate to national security and require consideration by the Cyber and Infrastructure Security Centre (CISC) in the Department of Home Affairs. The Bill would establish the role of CSC in the Department of Home Affairs and transfer the functions under Part 14 to the CSC. The Bill does not propose any new functions, but rather aligns the performance of the existing functions under Part 14 with the responsibilities of the Attorney General's Department and the Department of Home Affairs following changes to Administrative Arrangements in 2022. Currently the CAC (in the Attorney-General's Department) relies entirely on advice from the Department of Home Affairs to perform these functions, which is an inefficiency this measure will address.

The amendments would also enable the Attorney-General and the Minister for Home Affairs to specify, by legislative instrument, different persons or bodies, or classes of persons or bodies, to perform certain CAC and CSC functions as appropriate. This approach will support the timely and efficient discharge of CAC and CSC functions. For example, some routine and high-volume functions may be delegated to executive level officers within a Branch of the Attorney-General's Department or the Department of Home Affairs. Other functions of a particularly sensitive or complex nature may be reserved for performance by a particular Senior

[2] Australian Bureau of Statistics (December 2023) Characteristics of Employment, Australia, abs.gov.au, accessed 23 April, 2024.

Executive Service (SES) officer. The legislative instruments made by the Attorney General and Minister for Home Affairs will be subject to review and may be disallowed.

Schedule 5 – Information sharing between integrity agencies and oversight bodies

This schedule would amend the TIA Act to enhance the ability of specific bodies which oversee integrity agencies to properly scrutinise and audit interception activities and assure the public that integrity agencies are acting within the law.

The role of the state and territory oversight bodies is to oversee the operation of their respective integrity bodies to ascertain if any corruption, misconduct, unreasonable delays or invasions of privacy have occurred in their conduct. This is achieved by way of a range of functions including the audit, assessment, investigation and inspection of integrity agencies.

Currently, the oversight-body-specific permitted purposes set out under subsection 5(1) are focused on investigating misconduct and offences, and reporting on such investigations, and do not include the routine oversight function of each of the inspecting bodies. The amendments will expand the definition of 'permitted purpose' under subsection 5(1) of the TIA Act to align with the definition within the oversight bodies' respective enabling legislation to accurately encompass their oversight functions. The amendments also expand the scope of purposes for which the integrity agencies and oversight bodies are able to share interception information and interception warrant information under section 68 of the TIA Act to include sharing for the purposes of their oversight functions.

The amendments in this schedule apply to the:

- Inspector of the Independent Commission Against Corruption (NSW)
- Inspector of the Law Enforcement Conduct Commission (NSW)
- Inspector of the Independent Commission Against Corruption (SA)
- Parliamentary Inspector of the Corruption and Crime Commission (WA), and
- Victorian Inspectorate.

This schedule would also amend the TIA Act to include the South Australian Inspector of the Independent Commission Against Corruption as it absorbed the functions of the former reviewer of the Independent Commissioner Against Corruption in 2022. The inclusion of the South Australian Inspector of the Independent Commission Against Corruption in the TIA Act specifies the entirety of its oversight functions to enable it to lawfully receive interception information and interception warrant information to scrutinise and audit the interception activities of the South Australia Independent Commission Against Corruption and ensure it complies with its obligations under the TIA Act.

Lastly, Schedule 5 makes minor amendments to specify the jurisdiction of each integrity agency and oversight body where referred to in the TIA Act. As outlined above, these amendments to subsection 110A(1) have been specifically referred to the Committee by the Attorney-General as required by subsection 110A(11) of the TIA Act. The amendments do not change, or otherwise alter, the existing powers available to these agencies under the TIA Act.