The Centre for Public Integrity

Dr Catherine Williams
Executive Director

Professor Gabrielle Appleby
Research Director

Committee Secretary
Senate Legal and Constitutional Affairs Committee
PO Box 6100
Parliament House
Canberra ACT 2600

By email: legcon.sen@aph.gov.au

7 May 2026

Dear Secretary

Re: Secrecy Provisions Amendment (Repealing Offences) Bill 2026

The Centre for Public Integrity is an independent, non-partisan think tank dedicated to strengthening Australia's democratic institutions, with a particular focus on integrity, accountability and the rule of law. The Centre's work draws on multidisciplinary expertise in public law, governance and anti-corruption, and includes research, policy development and advocacy on transparency and integrity frameworks.

The Centre has previously engaged with the secrecy laws reform process, having made a submission to the Attorney-General's Department's Secrecy Provisions Review prior to the introduction of this Bill on 13 May 2023.

The Centre welcomes the Government's Commitment to Reform in this Area

The Centre welcomes the Government's introduction of the *Secrecy Provisions Amendment (Repealing Offences) Bill 2026,* and commends its commitment to progressing reform in this important area. Ensuring that Commonwealth secrecy provisions are appropriately framed is essential to maintaining public trust, supporting accountability, and strengthening Australia's system of open and responsible government.

The Centre for Public Integrity has long advocated for secrecy laws that are carefully confined to circumstances in which they are genuinely necessary to protect essential public interests. As a general principle, secrecy is in tension with the ideals of open government. While there will inevitably be circumstances in which confidentiality is required, this must be the exception rather than the rule. Where secrecy offences extend beyond what is strictly necessary, they risk entrenching a culture of unnecessary secrecy and undermining transparency, accountability, and democratic oversight.

The Centre is concerned that the retention or creation of secrecy offences in circumstances where they are not clearly justified may have a chilling effect on information-sharing and public accountability. For this reason, the Centre supports the approach taken by the Australian Law Reform Commission in its 2009 report, *Secrecy Laws and Open Government in Australia*, particularly the principled framework it articulated for assessing the necessity and scope of both general and specific secrecy offences.

Transparency about Implementing Prior Recommendations

In the interests of transparency, the Centre for Public Integrity has undertaken its own detailed analysis of the key inquiries and reviews on which this Bill draws, including the Australian Law Reform Commission's 2009 report, the Attorney-General's Department's 2023 Secrecy Review, and the Independent National Security Legislation Monitor's 2024 review, to assess the extent to which their recommendations have been implemented. This is attached for the Committee's Review at **Appendix A**.

That analysis indicates that the Government has, in large part, given effect to a substantial number of those recommendations, and should be commended for progressing reform at this scale.

At the same time, a number of recommendations have been only partially implemented or not implemented. Concerns about the consequences of this partial implementation have been raised in other submissions to this inquiry, including for instance by the Independent National Security Legislation Monitor.

It is important that there is transparency and accountability as to how, and to what extent, the work of such inquiries is taken forward. These processes involve significant public resources and play a critical role in informing law reform. While we raise these issues in the context of this Bill, they reflect a broader need for clearer public reporting and accountability mechanisms in relation to the implementation of recommendations arising from major reviews and inquiries.

Concerns remain regarding executive control over disclosure in integrity legislation

The Centre for Public Integrity reiterates the concerns it raised in its 2023 submission regarding executive control over disclosure in integrity legislation. These concerns have not been addressed by the Bill.

In our 2023 submission, we looked at section 47 of the *Auditor-General Act 1997* (Cth). That provision enables the Attorney-General to issue a certificate preventing the Auditor-General from including certain information in a report to Parliament on the basis that disclosure would be contrary to the public interest. As the Centre previously submitted, this mechanism raises significant rule of law and accountability concerns. It permits the executive to limit what is disclosed to Parliament by an independent officer, in circumstances where the information may go directly to matters of public administration and integrity.

This issue does not arise in isolation. Comparable provisions exist in Commonwealth integrity legislation which enable the executive to control, or significantly constrain, the disclosure of information obtained by independent oversight bodies. Most notably, section 235 of the *National Anti-Corruption Commission Act 2022* (Cth) empowers the Attorney-General to issue certificates preventing disclosure of information on public interest grounds, with significant legal consequences.

In the Centre's view, section 47 of the *Auditor-General Act*, and other equivalents in other integrity legislation, risks undermining the institutional independence of these bodies and the Parliament's ability to scrutinise executive government. It places the ultimate control over disclosure in the hands of the executive, without sufficient transparency or safeguards, and without requiring public justification of the decision. This creates the potential for overreach and is inconsistent with the principle that secrecy should be confined to what is strictly necessary to protect essential public interests.

The Centre's detailed analysis of these issues is set out in its 2023 submission, which is **attached** as **Appendix B** for the Committee's consideration.

Yours sincerely

Dr Catherine Williams

Executive Director
Centre for Public Integrity

Professor Gabrielle Appleby

Research Director
Centre for Public Integrity

About The Centre for Public Integrity

The Centre for Public Integrity is an independent think tank dedicated to preventing corruption, protecting the integrity of our accountability institutions, and eliminating the undue influence of money in politics in Australia. Board members of the Centre include the Hon Anthony Whealy KC, the Hon Margaret White AO, the Hon Michael Barker KC, Emma Mapl- Brown, Professor Allan Fels AO, Professor Joo Cheong Tham, and Geoffrey Watson SC.

More information at: www.publicintegrity.org.au

Appendix A
Overview of Bill and Implementation of Recommendations

Summary of the Secrecy Provisions Amendment (Repealing Offences) Bill 2026 (Cth)

The Bill comprehensively reforms how the Commonwealth protects government information. It tries to strike a balance between two competing interests: protecting sensitive information from harmful disclosure, and ensuring that secrecy laws do not unnecessarily chill free expression or press freedom.

The centrepiece of the Bill is the replacement of the existing general secrecy offence. Under current law, any breach by a Commonwealth officer of any of the more than 300 non-disclosure duties scattered across Commonwealth legislation automatically constitutes a criminal offence.[1] The Bill repeals this broad provision and replaces it with a narrower, targeted offence.[2]

The new offence only criminalises conduct where three conditions are satisfied: the person used or communicated information obtained through their Commonwealth role; they did so with the intention of obtaining a benefit or causing detriment to any person or Commonwealth entity; and it would be reasonable to conclude that the conduct was improper.[3] Importantly, the offence is extended beyond formal employees and contractors to capture persons providing voluntary or unpaid services to Commonwealth entities.[4]

A significant practical effect of the Bill is the removal of criminal liability from over 300 existing secrecy provisions. Most of these are converted into civil non-disclosure duties only, meaning breaches will be dealt with through administrative or disciplinary processes rather than criminal prosecution.[5]

The Bill introduces a new requirement that the Attorney-General give written consent before proceedings may be commenced against a person acting in a professional journalistic capacity, or as administrative staff of a news organisation, for any secrecy offence.[6] While arrest, charge and remand may still occur without consent, no further steps in proceedings may be taken until consent is obtained.[7]

Schedule 4 implements the Government's response to the Independent National Security Legislation Monitor's 2024 review and makes several important refinements to the existing Criminal Code offences.

The definition of 'cause harm to Australia's interests' is amended to apply a single, consistent threshold of 'prejudice' across all categories of protected interest, including national security, defence, international relations and public health and safety.[8] The definition of 'deal' is also narrowed to remove unsolicited receipt of information, ensuring that a person who inadvertently receives sensitive material does not thereby commit an offence.[9]

---

[1] Criminal Code Act 1995 (Cth) s 122.4 (as currently in force); Explanatory Memorandum, Secrecy Provisions Amendment (Repealing Offences) Bill 2026 (Cth) [5].
[2] Secrecy Provisions Amendment (Repealing Offences) Bill 2026 (Cth) sch 1 cl 1.
[3] Ibid sch 1 cl 1 (substituted s 122.4(1)(a)–(d)).
[4] Ibid sch 1 cl 1 (substituted s 122.4(1)(b)(iii)); Explanatory Memorandum, Secrecy Provisions Amendment (Repealing Offences) Bill 2026 (Cth) [20].
[5] Explanatory Memorandum, Secrecy Provisions Amendment (Repealing Offences) Bill 2026 (Cth) [10].
[6] Ibid sch 3 cl 2 (inserted s 123.6(1)).
[7] Ibid sch 3 cl 2 (inserted s 123.6(2)).
[8] Ibid sch 4 cll 1–4 (amending definition of 'cause harm to Australia's interests' in s 121.1(1)).
[9] Ibid sch 4 cl 5 (substituted definition of 'deal' in s 121.1(1)); Explanatory Memorandum, Secrecy Provisions Amendment (Repealing Offences) Bill 2026 (Cth) [253]–[254].

Appendix A
Overview of Bill and Implementation of Recommendations

Security classification under government policy is removed as a standalone element of the offences, addressing rule of law concerns that policy frameworks can be changed at any time without parliamentary oversight.[10] The aggravated offence is tightened so that it applies only where the offender held the highest level of security clearance, or committed the underlying offence with intention or knowledge of harm – replacing a broader set of aggravating circumstances that were considered arbitrary.[11]

For non-officials — such as journalists and members of the public who receive leaked information — the Bill reduces the maximum penalty from five to three years imprisonment[12] and repeals the offence of merely 'dealing with' sensitive information, confining non-official liability to active communication only.[13]

Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia* (Report 112, 2009)

ALRC Recommendation (Report 112, 2009)	**Extent of Incorporation into Bill**	**Status**
Rec 4-1: Repeal ss 70 and 79(3) of the Crimes Act 1914 (Cth) and replace them with a new general secrecy offence and subsequent disclosure offences in the Criminal Code.	Substantially incorporated. Sections 70 and 79 were replaced by the Part 5.6 Criminal Code offences enacted in 2018 (prior to this Bill). The Bill now replaces the existing general offence in s 122.4 with a new targeted offence (Sch 1, cl 1) and refines the non-official subsequent disclosure offence in s 122.4A (Sch 4, cl 22–24). The structural recommendation to relocate general secrecy offences to the Criminal Code has been fully implemented.	Incorporated.
Rec 5-1: The general secrecy offence should require that disclosure did, was reasonably likely to, or was intended to: (a) damage security, defence or international relations; (b) prejudice criminal justice; (c) endanger life or physical safety; or (d) prejudice public safety.	The new targeted offence in s 122.4 (Sch 1, cl 1) does not require harm to public interests — it requires intention to obtain a benefit or cause detriment.	Not incorporated.
Rec 5-2: Define 'security' and 'international relations' by reference to the ASIO Act 1979 (Cth) and the National Security Information Act 2004 (Cth).	Incorporated. The Bill amends the definition of 'cause harm to Australia's interests' to adopt the definition of 'security' from the ASIO Act (Sch 4, cl 4), replacing the previous 'security or defence of Australia' definition.	Incorporated.

[10] Secrecy Provisions Amendment (Repealing Offences) Bill 2026 (Cth) sch 4 cl 6; Explanatory Memorandum, Secrecy Provisions Amendment (Repealing Offences) Bill 2026 (Cth) [262].
[11] Secrecy Provisions Amendment (Repealing Offences) Bill 2026 (Cth) sch 4 cl 20 (substituted s 122.3(1)(b)); Explanatory Memorandum, Secrecy Provisions Amendment (Repealing Offences) Bill 2026 (Cth) [303].
[12] Secrecy Provisions Amendment (Repealing Offences) Bill 2026 (Cth) sch 4 cl 23 (amended s 122.4A(1) penalty).
[13] Ibid sch 4 cl 24 (repealing s 122.4A(2)).

Appendix A
Overview of Bill and Implementation of Recommendations

Rec 6-1: The general secrecy offence should regulate 'Commonwealth officers', including APS employees, contractors, contracted service providers and others in an employment or appointment relationship with the Commonwealth.	Substantially incorporated, and extended. The existing definition of 'Commonwealth officer' in s 121.1 broadly reflects the ALRC's recommended categories. The Bill goes further, extending the offences to persons providing paid or unpaid services to a 'Part 5.6 Commonwealth entity' (Sch 1, cl 1, 3–8).	Incorporated.
Rec 6-1: The general secrecy offence should regulate the disclosure of 'Commonwealth information' as defined in Rec 6–3.	Substantially incorporated. The offences in Part 5.6 apply to information 'made or obtained' by reason of a person's Commonwealth role, which is functionally equivalent to the ALRC's proposed definition of Commonwealth information. The new s 122.4 (Sch 1, cl 1) adopts similar language.	Incorporated.
Rec 6-3: The general secrecy offence should apply to any information to which a person has, or had, access by reason of being, or having been, a Commonwealth officer.	Incorporated. New s 122.4(1)(b) requires that information was 'made or obtained' by reason of the person being or having been a Commonwealth officer or otherwise engaged/providing services to a Part 5.6 Commonwealth entity.	Incorporated.
Rec 6-4: The general secrecy offence should require intention as the fault element attaching to disclosure.	Incorporated. For the new s 122.4 offence, the fault element for the conduct element (use or communication) is intention, consistent with this recommendation.	Incorporated.
Rec 6-5: The general secrecy offence should require knowledge, intention or recklessness as to whether disclosure would harm one of the specified public interests.	Not incorporated. The new targeted offence in s 122.4 (Sch 1, cl 1) does not require any fault element relating to harm to public interests – liability turns on improper use for benefit or detriment, not on harm to named public interests.	Not incorporated.
Rec 6-6: New Criminal Code offence for subsequent unauthorised disclosure by a non-official (B) who knows the original disclosure was in breach of the general secrecy offence, and knows/intends/is reckless as to harm.	Partially incorporated. Section 122.4A addresses non-official subsequent disclosures. The Bill refines this offence by: removing security classification as a standalone element (Sch 4, cl 22); reducing the penalty from 5 to 3 years (Sch 4, cl 23); and repealing the 'dealing with' offence for non-officials (Sch 4, cl 24), confining liability to communication. However, as is, there is fault element (i.e. no need for defendant to 'knows/intends/is reckless as to harm').	Partially incorporated.
Rec 6-7: New Criminal Code offence for subsequent unauthorised disclosure where information was disclosed on terms of	Partially incorporated. Section 122.4A captures some of this conduct where information was communicated by a Commonwealth official. However, the Bill does not introduce a free-standing 'breach of confidence' trigger for the non-official offence. The new s 122.4 targets improper use for benefit/detriment rather than breach	Partially incorporated.

Appendix A
Overview of Bill and Implementation of Recommendations

confidence, and B knows this and knows/intends/is reckless as to harm.	of confidence specifically. The ALRC's confidence-based trigger is only indirectly addressed.	
Rec 7-1: The general secrecy offence should include exceptions for: (a) disclosure in the course of duties; (b) ministerially authorised public interest disclosure; (c) disclosure of information already lawfully in the public domain.	Already incorporated. Section 122.5 of the Criminal Code provides a comprehensive set of defences.	Incorporated.
Rec 7-2: The subsequent disclosure offences should include an exception for disclosure of information already lawfully in the public domain.	Already incorporated. Section 122.5 defences apply to all Part 5.6 offences including the non-official offence in s 122.4A. The Bill does not disturb this.	Incorporated.
Rec 7-3: Public interest disclosure legislation should protect individuals subject to the general secrecy offence, subsequent disclosers, and those subject to confidential disclosure offences.	N/A. The Public Interest Disclosure Act 2013 (Cth) addresses this.	N/A
Rec 7-4: The general secrecy offence should carry a maximum penalty of 7 years imprisonment or 420 penalty units, or both.	Partially incorporated. The principal offences in ss 122.1 and 122.2 carry 7 years imprisonment (pre-existing, maintained by the Bill). However, the new s 122.4 targeted offence carries 2 years.	Partially incorporated.
Rec 7-5: Subsequent disclosure offences should carry a maximum penalty of 7 years imprisonment or 420 penalty units, or both.	Partially incorporated. The Bill reduces the maximum penalty for the non-official subsequent disclosure offence in s 122.4A from 5 to 3 years (Sch 4, cl 23), which is less than the ALRC's recommended 7 years.	
Rec 7-6: The offences should empower courts to grant injunctions to restrain actual or threatened disclosure.	Not incorporated. The Bill does not introduce an injunctive relief mechanism in connection with the secrecy offences.	Not incorporated.
Rec 8-1: Specific secrecy offences are only warranted where necessary and	Arguably incorporated. The Bill's entire rationale rests on this principle. More than 300 specific secrecy provisions lose criminal liability. The EM confirms each	Incorporated.

Appendix A
Overview of Bill and Implementation of Recommendations

proportionate to protecting essential public interests of sufficient importance to justify criminal sanctions.	retained offence was assessed against necessity and proportionality criteria.	
Rec 8-2: Specific secrecy offences should include an express harm requirement, except where the offence covers a narrowly defined category of information or the harm is to the trust relationship between individuals and government.	There are only 16 preserved non-disclosure duties under s 122.4 as a result of this Bill. Their nature is not affected by this Bill.	N/A
Rec 8-3: Specific secrecy offences should differ in significant and justifiable ways from the general secrecy offence.	Incorporated. Retained specific offences (e.g., under the Archives Act, Competition and Consumer Act, Patents Act) protect narrowly defined categories of information with distinct regulatory rationales, distinguishing them from the general Criminal Code offences.	Incorporated.
Rec 9-1: Specific secrecy offences applying to non-Commonwealth officers should clearly identify the parties regulated.	No change here.	N/A
Rec 9-2: Specific secrecy offences applying to current Commonwealth officers should also apply to former officers.	Incorporated. The general offences in ss 122.1, 122.2, 122.4, and 122.4A consistently apply to persons who 'are, or have been' Commonwealth officers or in equivalent roles. The Bill preserves and extends this to service providers (Sch 1, cl 1).	Incorporated.
Rec 9-3: Specific secrecy offences should not extend to conduct other than disclosure (e.g., making a record, receiving or possessing information) unless such conduct would cause harm to an essential public interest.	Partially incorporated. The Bill repeals the 'dealing with' offence for non-officials in s 122.4A(2) (Sch 4, cl 24), directly implementing this recommendation for non-officials. For officials, the 'dealing with' offences in ss 122.1(2) and 122.2(2) are retained but refined, with 'receiving' and 'obtaining' removed from the definition of 'deal' (Sch 4, cl 5).	Partially incorporated.
Rec 9-4: Specific secrecy offences should generally require intention as the fault element for the conduct element; strict liability should not attach to the conduct element.	No incorporated.	Not incorporated.

Appendix A
Overview of Bill and Implementation of Recommendations

Rec 9-5: Specific secrecy offences with an express harm requirement should require knowledge, intention or recklessness as to harm.	Incorporated. Sections 122.1 and 122.2, which contain express harm elements, apply recklessness to the harm-related fault elements, consistent with this recommendation. The Bill refines these fault elements in the aggravated offence provision (Sch 4, cl 20), requiring knowledge or intention for aggravated liability.	Incorporated.
Rec 9-6: Specific secrecy offences without a harm requirement should require knowledge or recklessness as to whether information falls within the protected category; strict liability should not apply.	Incorporated. The Bill removes security classification as a standalone element of offences (Sch 4, cll 6, 9–11), eliminating strict liability for classification status. Fault elements of recklessness apply to remaining circumstance elements.	Incorporated.
Rec 9-7: Subsequent disclosure offences should require knowledge or recklessness that the information was disclosed in breach of a secrecy offence, and knowledge, intention or recklessness as to harm.	Partially incorporated. The non-official offence in s 122.4A requires recklessness as to whether the communication would cause serious damage to security, defence or intelligence functions (Sch 4, cl 22). It does not require that they know the original disclosure was in breach – only that the communicated information meets specified criteria.	Partially incorporated.
Rec 9-8: Maximum penalties should reflect the seriousness of potential harm and fault elements.	Arguably incorporated. The Bill calibrates penalties to culpability: officials face 7 years (ss 122.1, 122.2), the new improper use offence carries 2 years (s 122.4), and non-officials face 3 years (s 122.4A as amended by Sch 4, cl 23). The aggravated offence (s 122.3) is tightened to apply only where culpability is clearly elevated (Sch 4, cl 20).	Incorporated.
Rec 9-9: Specific secrecy offences should not prescribe penalties different from those arising under the Crimes Act 1914 (Cth) formulae, or penalties that would apply to summary proceedings on indictable offences, without justification.	Incorporated. Schedule 2 repeals and decriminalises provisions whose penalties were identified as anomalous or disproportionate. Retained offences and new penalties (e.g., Business Names Registration Act 2011 (Cth) s 62M as amended by Sch 5, cl 1) are calibrated to align with the Criminal Code standard.	Incorporated.
Rec 10-1: Where a specific secrecy offence is repealed or amended, consideration should be given to retaining provisions codifying authorised information handling.	Incorporated. Schedule 2 Part 2 converts secrecy offences into non-disclosure duties without criminal liability rather than repealing them outright, preserving the information-handling obligations while removing disproportionate criminal sanctions.	Incorporated.

Appendix A
Overview of Bill and Implementation of Recommendations

Rec 10-2: Specific secrecy provisions imposing obligations on officers should generally include an exception for disclosures in the course of functions or duties.	Incorporated. Section 122.5(1) provides a defence for disclosures in the course of functions or duties, applying to all Part 5.6 offences. Retained specific offences generally include equivalent exceptions.	Incorporated.
Rec 10-3: Specific secrecy offences should not apply to information that is lawfully in the public domain.	Incorporated. Section 122.5 defences include a prior public domain exception. The Bill does not disturb this.	Incorporated.
Rec 10-4: Exceptions and defences should be framed consistently with the Guide to Framing Commonwealth Offences.	Incorporated. The EM cites the Guide to Framing Commonwealth Offences throughout.	Incorporated.
Rec 10-5: Public interest disclosure legislation should, where possible, protect individuals subject to specific secrecy offences.	Out of scope. This recommendation concerns the Public Interest Disclosure Act 2013 (Cth), which is not amended by the Bill. The Bill's reduction of criminal liability indirectly broadens protection for potential disclosers.	N/A
Rec 11-1: Government agencies should review specific secrecy offences to determine: (a) whether criminal sanction is warranted; (b) whether the offence complies with best practice principles; and (c) whether consolidation is appropriate.	Incorporated. The 2023 AGD Secrecy Review and the subsequent legislative program directly implement this recommendation at scale. The Bill enacts the outcomes of that review, removing or decriminalising more than 300 provisions identified as no longer warranting criminal sanction.	Incorporated.
Rec 11-2: The AGD should incorporate guidance on best practice secrecy offence principles into the Guide to Framing Commonwealth Offences.	N/A	N/A
Rec 12-1: Amend reg 2.1(3) of the Public Service Regulations 1999 (Cth) to apply to information where disclosure is reasonably likely to prejudice the effective working of government.	N/A	N/A

Appendix A
Overview of Bill and Implementation of Recommendations

Rec 12-2: The APS Commission should amend the APS Values and Code of Conduct in Practice to provide guidance on 'reasonably likely to prejudice the effective working of government'.	N/A	N/A
Rec 12-3: Remove the express prohibition on disclosure of confidential information in reg 2.1(4) of the Public Service Regulations.	N/A	N/A
Rec 12-4: Agency information-handling policies should set out disciplinary penalties that may result from breaching secrecy obligations.	N/A. Indirectly relevant given the Bill's shift toward administrative rather than criminal consequences for many breaches.	N/A
Rec 13-1: Agencies employing persons other than under the Public Service Act should adopt reg 2.1 requirements and equivalent safeguards in employment terms.	N/A	N/A
Rec 13-2: Agencies should remind employees on termination of their continuing liability under the general secrecy offence and relevant specific offences.	N/A	N/A
Rec 13-4: Private sector organisations performing services for government under contract should ensure employees are aware of secrecy obligations.	N/A	N/A
Rec 13-5: Government should include secrecy requirements equivalent to those on employees in terms of appointment for board and committee members.	The extension of secrecy offences to persons providing paid or unpaid services (including advisory board members) in the new s 122.4 (Sch 1, cl 1) addresses the gap this recommendation identified – advisory board members are now expressly within the criminal framework.	Incorporated.

Appendix A
Overview of Bill and Implementation of Recommendations

Red 13-6: Board and committee members with access to Commonwealth information should be made aware of their secrecy obligations.	N/A. Administrative recommendation.	N/A
Rec 14-1: Agencies should develop information-handling policies setting out what can be disclosed, what requires authorisation, and what could lead to disciplinary action or criminal prosecution.	N/A	N/A
Rec 14-2: Agencies should make information-handling policies publicly available, except where impractical or unreasonable.	Partially incorporated. The Bill inserts a new s 41D into the Intelligence Services Act 2001 (Cth) requiring publication of the DIO Mandate (Sch 4, cl 46), implementing the principle of publicly available agency information-handling frameworks for at least one intelligence agency. This is narrower than the ALRC's recommendation.	Partially incorporated.
Rec 14-3: Agencies should review secrecy directions to ensure consistency with the implied constitutional freedom of political communication.	N/A	N/A
Rec 14-4: Agencies that regularly share information with other agencies should enter into MOUs setting out terms and conditions for information exchange, and make these publicly available.	N/A	N/A
Rec 14-5: Agencies should implement ICT systems to facilitate secure and convenient handling of Commonwealth information.	N/A	N/A
Rec 15-1: Agencies should develop training programs on information-handling obligations, including whistleblowing channels.	N/A	N/A

Appendix A
Overview of Bill and Implementation of Recommendations

Rec 15-2: Agencies administering oaths or affirmations of secrecy should ensure these properly reflect relevant secrecy laws.	N/A	N/A
Rec 15-3: Agency information-handling policies should set out how employees can raise concerns about their obligations.	N/A	N/A
Rec 15-4: The Information Commissioner should review and report on agency information-handling policies.	N/A	N/A
Rec 16-1: Section 38 of the FOI Act 1982 (Cth) should be amended to include a definitive list of secrecy provisions providing exemptions from disclosure obligations.	Not incorporated.	Not incorporated.
Rec 16-2: Explanatory memoranda for legislation adding secrecy provisions to the FOI s 38 list should assess implications for open government.	N/A	N/A
Rec 16-3: Sections 91 and 92 of the FOI Act should be amended to extend indemnities to authorised FOI officers who disclose exempt documents in a bona fide exercise of discretion.	Not incorporated.	Not incorporated.
Rec 16-4: The FOI Act should be amended to expressly override non-disclosure obligations in other legislation.	Not incorporated.	Not incorporated.
Rec 16-5: Section 33(3) of the Archives Act 1983 (Cth) should be repealed.	Not incorporated.	Not incorporated.

Appendix A
Overview of Bill and Implementation of Recommendations

Rec 16-6: The Archives Act should be amended to provide that its public access provisions override any secrecy provisions that would otherwise apply.	Not incorporated.	Not incorporated.
Rec 16-7: A Privacy Impact Assessment should be conducted for proposed secrecy provisions that significantly detract from Privacy Act standards.	N/A. However, the EM addresses the Bill's compatibility with privacy rights under Art 17 ICCPR and notes the Privacy Act 1988 (Cth) continues to apply to personal information after decriminalisation of specific secrecy provisions.	N/A

Attorney-General's Department, *Review of Secrecy Provisions* (November 2023)

AGD Review of Secrecy Provisions (2023)	**Extent of Incorporation into Bill**	**Status**
Rec 1: • Principle 1: Secrecy offences should be limited to circumstances where there is an essential public interest that requires criminal sanctions. • Principle 2: Criminal liability for the protection of Commonwealth information should primarily be imposed through general secrecy offences. • Principle 3: Specific secrecy offences should apply where criminal liability differs in significant and justifiable ways from general secrecy offences. • Principle 4: A harms-based approach should be taken in framing secrecy offences. Secrecy provisions should: (1) contain an express	Partially incorporated. Principles 1–4 (necessity, primacy of general offences, harms-based approach): The Bill's core rationale reflects these principles. More than 300 provisions are decriminalised or repealed precisely because they could not satisfy Principle 1. The new s 122.4 offence (Sch 1, cl 1) introduces a targeted general offence. However, the new offence departs from a pure harms-based approach (Principle 4): it requires intention to obtain a benefit or cause detriment rather than harm to a public interest. Principle 5 is incorporated insofar that offences consistently apply to former officers (Sch 1, cl 1, 3–8). Principle 6 is incorporated given the non-official offence in s 122.4A is maintained as a separate provision. Principle 7 is incorporated as the Bill reduces non-official penalties (Sch 4, cl 23) and repeals the non-official dealing offence (Sch 4, cl 24), applying a higher threshold for non-official liability. Principle 8 is incorporated as the definition of 'deal' is clarified (Sch 4, cl 5) and dealing offences are removed for non-officials (Sch 4, cl 24). Principle 9 is already incorporated given recklessness applies to circumstance elements and intention to conduct elements. Principle 10 is incorporated as penalties are calibrated by culpability (see Sch 4, cl 23; Sch 5, cl 1). Principle 11 is incorporated thanks to existing s 122.5(6) journalism defence is preserved; new Attorney-General consent requirement for journalist prosecutions added (Sch 3, cl 2). Principle 12 (agency review): N/A.	Partially Incorporated.

Appendix A
Overview of Bill and Implementation of Recommendations

harm element, (2) cover a narrowly defined category of information and the harm to an essential public interest is implicit, or (3) protect against harm to the relationship of trust between individuals and the Government integral to the regulatory functions of government. • Principle 5: Secrecy offences that apply to Commonwealth officers should also apply to former Commonwealth officers. • Principle 6: Secrecy offences should clearly identify any third parties regulated by the offence and separate offences should apply to third parties. • Principle 7: Offences capturing third parties should have a higher threshold for establishing criminal liability. • Principle 8: Secrecy offences should clearly identify the conduct regulated. • Principle 9: Fault elements for secrecy offences should generally require intention or recklessness (awareness of a substantial risk) in line with the default approach in the Criminal Code Act 1995 (Criminal Code).		

Appendix A
Overview of Bill and Implementation of Recommendations

• Principle 10: Secrecy offences should have maximum penalties that reflect the potential seriousness of the conduct. • Principle 11: Offence-specific defences should be considered when framing secrecy offences, including to protect public interest journalism. • Principle 12: All Commonwealth departments and agencies should regularly review specific secrecy offences in legislation they administer as part of reviews of legislation and legislative instruments.		
Rec 2: Legislation be developed to repeal specific secrecy offences and non-disclosure duties identified through this Review's consultations as no longer being required.	Incorporated. This is the central legislative purpose of of the Bill. Schedule 2 Part 1 repeals secrecy offences and non-disclosure duties across 13 Acts and instruments that the AGD Secrecy Review identified as no longer required. Schedule 2 Part 2 additionally removes criminal liability from a further set of offences (e.g., in the Australian Jobs Act 2013 (Cth), Defence (Inquiry) Regulations 2018 (Cth), Reserve Bank Act 1959 (Cth), Torres Strait Fisheries Regulations 1985 (Cth)), converting these to civil non-disclosure duties only. The combined effect of Sch 2 and the repeal of old s 122.4 (Sch 1, cl 1) removes criminal liability from more than 300 provisions, directly implementing this recommendation.	Incorporated.
Rec 3: To enable the further reduction of specific secrecy offences and non-disclosure duties, the Attorney-General's Department develop a new general secrecy offence for inclusion in Part 5.6 of the Criminal Code to ensure Commonwealth officers and persons who	Partially incorporated. The Bill introduces a new general offence but departs significantly from the recommended harm standard. The Bill does introduce a new targeted general offence in s 122.4 (Sch 1, cl 1) that addresses improper use or communication of Commonwealth information. Like the AGD's recommendation, the new offence: applies to current and former Commonwealth officers (and extends to paid and unpaid service providers); focuses on use and communication of information obtained in a Commonwealth capacity; and does not require proof of actual harm (only of intention to obtain benefit or cause	Partially incorporated.

Appendix A
Overview of Bill and Implementation of Recommendations

perform services for or on behalf of the Commonwealth do not disclose information obtained in connection with their employment or the provision of the service, where that disclosure would be prejudicial to the effective working of Government or where the information was communicated to them in confidence.	detriment). However, the new offence departs from Rec 3 in one critical respect: it does not adopt the 'prejudicial to the effective working of government' harm standard, which the AGD Review recommended. The Attorney-General's second reading speech expressly acknowledged that the Government heard from stakeholders who told it that such a broad offence was not warranted, and elected instead to frame the offence around improper use for benefit or detriment. This represents a conscious policy decision to enact a narrower offence than recommended. The recommendation to capture persons who perform services for the Commonwealth – not merely formal employees and contractors – is, however, fully incorporated (new s 122.4(1)(b)(iii), Sch 1, cl 1).	
Rec 4: If Recommendation 3 is implemented, all Commonwealth departments and agencies identify which specific secrecy offences and non-disclosure duties may then be repealed.	Incorporated. The Bill is the product of precisely this process. Following the AGD Secrecy Review, all Commonwealth agencies assessed their specific secrecy provisions against the new general offence framework. The resulting legislative program is reflected in Schedule 2, which repeals or decriminalises provisions across a broad range of agency portfolios. The Explanatory Memorandum confirms that Schedule 2 provisions were identified through the AGD Secrecy Review process and subsequent government consultation as no longer requiring criminal liability in light of the new general offence framework.	Incorporated
Rec 5: Repeal section 122.4 of the Criminal Code, or allow it to sunset on 29 December 2024.	Incorporated. Schedule 1, item 1 of the Bill repeals existing s 122.4 and replaces it with a new targeted offence.	Incorporated.
Rec 6: Repeal the proper place of custody offences in sections 122.1(3) and 122.2(3) of the Criminal Code.	Incorporated. Schedule 4, items 17 and 19 repeal ss 122.1(3) and 122.2(3) respectively, directly implementing this recommendation.	Incorporated.
Rec 7: Improve protections for individuals providing information to Royal Commissions by: (a) amending the Royal Commissions Act 1902 (Cth) to establish a framework clarifying the application of secrecy offences to such individuals and appropriate protective security requirements;	N/A	N/A

Appendix A
Overview of Bill and Implementation of Recommendations

and (b) amending s 122.5 of the Criminal Code to include an additional defence where information is communicated for the purposes of a Royal Commission.		
Rec 8: Legislation be developed to apply a public interest journalism defence similar to the defence in s 122.5(6) of the Criminal Code to additional secrecy offences, to be identified through work following the Review	Partially incorporated. The Bill takes a different approach to this recommendation. Rather than extending the s 122.5(6) journalism defence to additional specific secrecy offences, the Bill introduces a new Attorney-General consent requirement for journalist prosecutions across all secrecy offences (new s 123.6, Sch 3, cl 2). The Explanatory Memorandum (at para 8) explains that the Government determined that the majority of specific secrecy offences did not apply to journalists, and that for those which could, the information protected was sufficiently sensitive that it would rarely be appropriate for disclosure outside established whistleblower frameworks. The existing s 122.5(6) defence for public interest journalism in Part 5.6 offences is preserved.	Partially incorporated.
Rec 9: Legislation be developed as a priority to require the protection of public interest journalism to be considered in decisions on warrant applications, including in the investigation of secrecy offences, as recommended by the Parliamentary Joint Committee on Intelligence and Security (PJCIS) in its 2020 Inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press.	Not incorporated.	Not incorporated.
Rec 10: The AGD amend the Commonwealth's Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers to include the 12 principles in Recommendation 1 and develop public	N/A	N/A

Appendix A
Overview of Bill and Implementation of Recommendations

information materials on the operation of Commonwealth secrecy offences.		
Rec 11: Request the Independent National Security Legislation Monitor (INSLM) consider, as part of its review of the National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018 (Cth), the appropriateness of the definitions of 'inherently harmful information' and 'cause harm to Australia's interests' in Part 5.6 of the Criminal Code.	Incorporated. The Government requested and received a dedicated INSLM review of Part 5.6 secrecy offences, which reported in June 2024 (the INSLM Secrecy Review). This review directly addressed both definitions identified in Rec 11. The Government's response accepted or agreed in principle to 12 of the 15 INSLM recommendations. The Bill gives effect to those accepted recommendations in Schedule 4. In particular: the definition of 'inherently harmful information' is narrowed by removing the security classification limb (Sch 4, cl 6); the definition of 'cause harm to Australia's interests' is refined to apply a single 'prejudice' threshold and to adopt the ASIO Act definition of 'security' (Sch 4, cl 1–4).	Incorporated.

INSLM, *Secrecy Review* (June 2024)

INSLM Secrecy Review (2024)	**Extent of Incorporation into Bill**	**Status**
Rec 1: The offences in Part 5.6 should not rely on information being classified under a policy framework as an element of the offence.	Incorporated. The Bill removes security classification as a standalone element from the deemed harm offence for officials in s 122.1 (Sch 4, cl 6), the non-official offence in s 122.4A (Sch 4, cl 22), and the aggravated offence in s 122.3 (Sch 4, cl 20). The definitions of 'security classification', 'security classified information' and 'security or defence of Australia' are all repealed (Sch 4, cll 9–11). Strict liability for classification-related elements is removed by the repeal of s 121.1(3) (Sch 4, cl 12).	Incorporated.
Rec 2: The deemed harm offences in s 122.1 should not apply to all information connected to an intelligence agency's functions. Instead, deemed harm should be limited to intelligence information (as defined) and the operations, capabilities, technologies, methods and sources used to obtain or communicate that information.	Partially incorporated. Rather than restricting 'inherently harmful information' to the INSLM's proposed narrower definition of intelligence information, the Bill removes the security classification limb from s 122.1 (Sch 4, cl 6) and retains the existing intelligence agency information limb in the definition of 'inherently harmful information' – covering information obtained or made by or on behalf of domestic or foreign intelligence agencies.	Partially incorporated.

Appendix A
Overview of Bill and Implementation of Recommendations

Rec 3: The deemed harm offences in s 122.1 should not apply to all information relating to the operations, capabilities or technologies of, or methods or sources used by, a domestic or foreign law enforcement agency. Instead, the deemed harm offence should be limited to information that relates to the technologies, capabilities and methods used to exercise special electronic surveillance powers.	Not incorporated. The Bill does not restructure the s 122.1 definition of 'inherently harmful information' to limit it to electronic surveillance capabilities as the INSLM recommended.	Not incorporated.
Rec 4: If separate general 'deemed harm' offences are to be retained in the Intelligence Services Act 2001 (Cth), the ASIO Act 1979 (Cth) and the ONI Act 2018 (Cth), those offences should be narrowed so that the scope of the deemed harm is no wider than that described in Recommendation 2, except that: for ASIS and ASIO, existing specific offences relating to the identity of current and former staff, affiliates and agents should be retained; and in the ASIO Act, the offence should include a category of information connected to the function of assessing and issuing Australia's highest level of security clearance.	Not incorporated.	Not incorporated.
Rec 5: The functions of the Defence Intelligence Organisation (DIO) should be set out in legislation or in a disallowable legislative instrument.	Partially Incorporated. Schedule 4, item 46 inserts a new s 41D into the Intelligence Services Act 2001 (Cth), requiring the Director of the DIO to make the Defence Intelligence Organisation Mandate publicly available as in effect from time to time, without giving it a statutory basis.	Partially Incorporated.

Appendix A
Overview of Bill and Implementation of Recommendations

Rec 6: The offence in s 122.2 should apply to disclosures of information by officials where there is harm or likely harm to: security, defence or international relations (as defined); the utility of operational and technical capabilities and methods connected to statutory powers granted to any agency to access information or to search people, places or things (other than those covered by s 122.1) to combat crime; AFP protective and custodial functions and proceeds of crime functions; or the health or safety of the Australian public or a section of the Australian public.	Partially incorporated. The Bill adopts the INSLM's single harm threshold of 'prejudice' across the s 122.2 categories (Sch 4, cl 1–4). The definition of 'security' is aligned with the ASIO Act (Sch 4, cl 4). The health/safety and AFP categories are retained with the standardised 'prejudice' threshold. However, the INSLM's recommended new category for operational and technical capabilities of agencies exercising statutory crime-fighting powers (other than those in s 122.1) is not expressly added as a separate category.	Partially incorporated.
Rec 7: The definition of 'deal with' for the purpose of Part 5.6 should be amended so that it excludes initial receipt and does not overlap with the disclosure offences. The remaining parts of the definition (collect, possess, record and copy) are broadly justified for officials, although some clarification in drafting is suggested.	Incorporated. The Bill substitutes a new definition of 'deal' in s 121.1(1) (Sch 4, cl 5) that: removes 'receiving or obtaining' from the definition (addressing the unsolicited receipt concern); removes 'communicating', 'publishing' and 'making available' (eliminating overlap with communication offences); and retains 'collects', 'possesses', 'makes a record of', 'copies', 'alters' and 'conceals'. This directly implements the INSLM's recommendation.	Incorporated.
Rec 8: The offence for 'dealing with' information by non-officials in s 122.4A(2) should be repealed.	Incorporated. Schedule 4, item 24 repeals s 122.4A(2), directly implementing this recommendation.	Incorporated.
Rec 9: The 'proper place of custody' offences in ss 122.1(3) and 122.2(3) should be repealed.	Incorporated. Schedule 4, items 17 and 19 repeal ss 122.1(3) and 122.2(3) respectively.	Incorporated.
Rec 10: The maximum penalty for offences by	Incorporated. Schedule 4, item 20 substitutes a new s 122.3(1)(b) which confines the aggravated offence to	Incorporated.

Appendix A
Overview of Bill and Implementation of Recommendations

officials under Part 5.6 should be increased only where, at the time the person received the information or committed the underlying offence, the person held the highest level of Australian Government security clearance; or where the person intended or knew their conduct would or was likely to cause a type of harm covered by the underlying offence.	three circumstances: (i) the person knew the information was inherently harmful information (for s 122.1 underlying offences); (ii) the person intended their conduct to cause or be likely to cause harm to Australia's interests (for s 122.2 underlying offences); and (iii) the person held the highest level of Australian Government security clearance at the relevant time (for any Part 5.6 offence). Three existing aggravating circumstances are repealed.	
Rec 11: Any general offence to replace s 122.4 should be consistent with the following principles: (1) apply to disclosures that prejudice the prevention, detection, investigation, prosecution or punishment of a criminal offence against a Commonwealth law; (2) be harm-based and relate to essential public interests, with any deemed harm limited to a very narrow category; (3) cover only disclosures that cannot be adequately dealt with by existing contractual and administrative remedies; (4) avoid broad and uncertain language such as 'functioning of government'; (5) apply to current and former Commonwealth officials and others performing work for a Commonwealth entity, closely linked to some contract, agreement or arrangement; and (6) the penalty for reckless conduct should be no	Partially incorporated. The new s 122.4 offence (Sch 1, cl 1) reflects several INSLM principles: principles (3) (the offence is targeted and supplementary to specific offences), (5) (it applies to current and former officials and service providers), and (6) (the penalty is 2 years: EM [13]). However, the new offence departs from Principles 1 and 2 in important respects. It does not adopt a harm-to-public-interests model, instead requiring intention to obtain a benefit or cause detriment. It does not expressly require that the disclosure prejudice the criminal justice system or any listed public interest. The INSLM's explicit warning against 'functioning of government' language (Principle 4) was heeded.	Partially incorporated.

Appendix A
Overview of Bill and Implementation of Recommendations

more than 2 years imprisonment.		
Rec 12: The offence in s 122.4A for communications by non-officials should be modified so that: (a) classification markings do not form an element of the offence; (b) the current requirement that actual harm be established should be maintained; and the offence should apply to: causing serious damage to security or defence of Australia (with those terms defined as per Rec 6); seriously undermining the utility of technologies, capabilities and methods used to exercise special statutory powers (per Recs 3 and 4); seriously impeding the prevention, detection, investigation, prosecution or punishment of a criminal offence; prejudicing the health or safety of the Australian public; and (c) the maximum penalty should be approximately half the maximum penalty for a comparable communication by an official. Action should also be taken to ensure that ABC and SBS staff and contractors are not inadvertently covered by the offences for officials.	Partially incorporated. The Bill implements each core element: (a) security classification is removed as an element (Sch 4, cl 22); (b) the actual serious damage requirement is maintained and the harm categories are refined to cover serious damage to security (ASIO Act definition), defence of Australia, and operations/capabilities/methods of intelligence agencies (Sch 4, cl 22), plus existing health/safety and criminal justice prevention categories; (c) the penalty is reduced from 5 to 3 years (Sch 4, cl 23); and ABC/SBS staff are excluded from the 'Part 5.6 Commonwealth entity' definition (Sch 1, cl 3; Sch 4, cl 3), ensuring they are treated as non-officials. The only partial element is the 'statutory powers' category in Rec 12(b)(ii): the INSLM recommended expressly covering the technologies, capabilities and methods used to exercise special electronic surveillance powers.	Partially incorporated.
Rec 13: A new general public interest defence or element should not be added in Part 5.6. However, consideration should be given to recasting the current	Not incorporated. The Government did not agree to recast the journalism defence in s 122.5(6) from a defence to an exception. The Bill retains s 122.5(6) as a defence (not an exception).	Not incorporated.

Appendix A
Overview of Bill and Implementation of Recommendations

defence for journalists as an exception rather than a defence.		
Rec 14: The requirement that the Attorney-General's consent be obtained for prosecution under Part 5.6 should be retained. The Attorney-General's consent should be required regardless of whether the prosecution proceeds by way of committal or summary proceedings.	Incorporated. Schedule 4, item 43 repeals and replaces s 123.5(1) with a new provision requiring Attorney-General's written consent for 'proceedings for an alleged offence against this Part', without the former limitation to committal proceedings.	Incorporated.
Rec 15: Consideration should be given to revising the Prosecution Policy of the Commonwealth to expressly include the public interest in a free and open press as one of the factors to be considered in any prosecution for a secrecy offence involving a journalist or news media organisation.	N/A. However, the Bill responds to the underlying concern through the new consent mechanism in Sch 3, cl 2 (new s 123.6), which requires the Attorney-General's written consent before proceedings can be commenced against a journalist or news organisation administrative staff member.	N/A

The Centre for Public Integrity

Dr Catherine Williams
Executive Director

Secrecy Review Team
Attorney-General's Department
By email: secrecyreview@ag.gov.au

12 May 2023

Dear

Review of Secrecy Provisions

Thank you for the opportunity to make a submission to your Department's Review of Secrecy Provisions.

The Centre for Public Integrity is an independent think tank made up of integrity experts from the judiciary, legal practice and academia. Our work is dedicated to preventing corruption, protecting the integrity of our accountability institutions, and eliminating the undue influence of money in politics in Australia.

Should you wish to discuss any matters raised in our attached submission, we would be pleased to assist.

Yours sincerely,

Dr Catherine Williams
Research Director
The Centre for Public Integrity

Review of Commonwealth Secrecy Provisions

Secrecy is anathema to open government. To recognise that is not to deny that there will be circumstances where secrecy is necessary; it does, however, follow that if open government is desirable, then secrecy must be limited to only the cases in which it is *genuinely* required to protect *essential* public interests.

We are concerned that the inclusion of secrecy offences where they are anything other than genuinely necessary to protect essential public interests reinforces a culture of government secrecy, and in so doing it has a deleterious impact upon efforts to achieve open government.

We support the recommendations of the Australian Law Reform Commission in its 2009 report *Secrecy Laws and Open Government in Australia* in respect of the principles which should guide the framing of general and specific secrecy offences. In respect of the latter (which we note for the purposes of this review includes non-disclosure duties which apply to current and former Commonwealth officers and attract criminal liability), one problematic duty is located at s 37 of the *Auditor-General Act 1997* (Cth). We have previously examined this provision as part of our submission to the 2020 review by the Joint Committee of Public Accounts and Audit (***JCPAA***) of the *Auditor-General Act 1997*
(Cth), and include it here as a case study illustrative of the difficulties non-disclosure provisions can generate; it is also of value in helping discern the principles that should guide the parameters of duties analogous to s 37, which have implications for our system of responsible government.

Case study: section 37 of the *Auditor-General Act 1997* (Cth)

1. UN Resolution 69/228 of 2014 acknowledges the role that Supreme Audit Institutions (***SAIs***), like the Auditor-General and Australian National Audit Office, play in "fostering governmental accountability for the use of resources and their performance in achieving development goals"[1] and encourages Member States to "give due consideration to the independence and capacity-building of supreme audit institutions in a manner consistent with their national institutional structures".2 It also encourages Member States to apply the Mexico Declaration on Supreme Audit Institutions' Independence of 2007 (Mexico Declaration).

[1] UN Resolution 69/228 of 2014, "Promoting and fostering the efficiency, accountability, effectiveness and transparency of public administration by strengthening supreme audit institutions" < https://undocs.org/en/A/RES/69/228 > accessed 20 January 2021.

2. A number of principles of the Mexico Declaration are directed at enshrining the independence of SAIs:

   - Principle 5 states that "SAIs should not be restricted from reporting the results of their audit work"; and
   - Principle 6 states that SAIs should be "free to decide the content of their audit reports, as well as to "make observations and recommendations in their audit reports" and to "publish and disseminate their reports, once they've been formally tabled or delivered to the appropriate entity".

3. Section 37(1) of the *Auditor-General Act 1997* (Cth) prevents the Auditor-General from including certain information in a public report. Section 37(3) goes further, and prevents this information from being disclosed to the Parliament, a member of the Parliament or a committee of the Parliament.

4. In the course of the ANAO audit which culminated in the report *Auditor-General's Report No. 6 of 2018-19: Army's Protected Mobility Vehicle – Light*, the then-Attorney General issued a certificate under s 37(1) of the Act requiring that certain information be omitted from the Auditor-General's report. Auditor-General Hehir has described this incident in the following terms:

> *The certificate included omission of parts of the audit conclusion in the report and, as a result of this, I was prevented from fully concluding against the audit objective – which was 'to assess the effectiveness and value for money of Defence's acquisition of light protected vehicles'. This resulted in, for the first time, an ANAO performance audit being tabled with a disclaimer of conclusion to the effect that I was not able to prepare a report that expressed a clear conclusion on the audit objective in accordance with the ANAO Auditing Standards*.[3]

[2] Ibid.

[3] Australian National Audit Office, "*Annual report 2018-19*" https://www.anao.gov.au/work/annual-report/anao-annual-report-2018-19 accessed 4 December 2020.

5. At the time, Auditor-General Hehir described this not only as the most significant issue for 2018-19, but also as the most significant in his time as Auditor-General.[4]

6. That the issue arose after Thales Australia Limited applied to the Attorney-General to have a certificate issued under s 37(1)(b) on the ground that the inclusion of particular information in the public audit report "would unfairly prejudice the commercial interests of any body or person" is particularly alarming.[5]

7. On 9 December 2020, the Administrative Appeals Tribunal granted Senator Rex Patrick's Freedom of Information review application in respect of the redacted report.[6] The unredacted version, which is now publicly available, reveals that sections which had been redacted following the issuing of the s 37 certificate include confirmation that the ANAO informed Defence in August 2017 of its preliminary finding that the Hawkei did not appear to represent value for money when compared to the Joint Light Tactical Vehicle,[7] as well as the conclusion that "defence has not clearly demonstrated that the acquisition provides value for money, as it did not undertake robust benchmarking in the context of a sole-source procurement".[8] How these issues are capable of affecting the Commonwealth's security, defence or international relations – one of the bases upon which the s 37 certificate was issued – remains unclear.

8. The Centre for Public Integrity considers that the certification process provided for by s 37 is, in its current form, capable of compromising the ability of the Auditor-General to effectively fulfil their mandate of providing independent, accurate advice to the Parliament to aid in accountability and transparency of public sector.

[4] Australian National Audit Office, "*Annual report 2018-19*" https://www.anao.gov.au/work/annual-report/anao-annual-report-2018-19 accessed 4 December 2020.

[5] Auditor-General submission to Senator Dean Smith 4 October 2018.

[6] *Patrick and Secretary, Department of Prime Minister and Cabinet (Freedom of information)* [2020] AATA 4964 (9 December 2020).

[7] Unredacted version of "*Auditor-General Report No. 6 2018-19 – Army's Protected Mobility Vehicle – Light*" at 68.

[8] Ibid at 6.

9. We note that concerns regarding the operation of this certification process are not novel. In Report 346 of 1996, the Joint Committee of Public Accounts (predecessor to the JCPAA) at Recommendation 9 urged that the Auditor-General Bill should provide that:

> *"(a) the Executive may only direct the Auditor-General to exclude sensitive audit information from a report to the Parliament where disclosure of the information would be likely to prejudice national security;*
>
> *(b) where the Executive orders the Auditor-General to suppress sensitive audit information on the grounds of national security, the Audit Committee should receive an unabridged copy of the audit report and/or a copy of the suppressed information; and*
>
> *(c) where sensitive information is excluded from an audit report, the fact of the exclusion and the reasons for the exclusion should be reported to the Parliament in the audit report."*

10. We further note that the JCPAA in Recommendation 3 of its Report 478 recommended that the following issues, raised by the Auditor-General in his submission to the Inquiry which was the subject of that Report, be referred for further consideration in this current review:

- whether there should be provision for a confidential report to be provided to at least the Chair of the JCPAA, along with relevant Ministers;
- whether the JCPAA should be consulted on a confidential basis if a proposed certificate affects the audit conclusion or information not otherwise prohibited from disclosure;
- whether there should be a distinction between types of certificates and at least a requirement for confidential consultation with the JCPAA before certificates are issues for non-national security matters; and
- whether substantive reasons should be provided when a certificate is issued.

11. The JCPAA, in its March 2022 Report following the 2020 review (Report 491), recommended that these amendments be made.

12. The Centre for Public Integrity strongly endorses the adoption of all of these measures: they are essential for promoting transparency in respect of s 37 certificates. We also consider that the JCPA's 1996 recommendation that the Executive may only direct the Auditor-General to exclude sensitive audit information from a report to the Parliament where disclosure of the information would be likely to prejudice national security, should be given serious consideration: the interests of the Australian people in knowing how public monies have been spent cannot justifiably be subordinated to – for example – a claim by a private organisation that its commercial interests (howsoever defined) would be affected by the Australian Parliament receiving certain information.

13. Insofar as the Auditor-General is mandated to report to the Parliament rather than the Executive, and the Parliament is constitutionally empowered to scrutinise the Executive, the prohibition contained at s 37(3) of the Act (preventing the Auditor-General from disclosing to a House of the Parliament, a member of the Parliament, or a parliamentary committee, information that s 37(1) prohibits being included in a public report) should also be removed, or its application amended.

About The Centre for Public Integrity

The Centre for Public Integrity is an independent think tank dedicated to preventing corruption, protecting the integrity of our accountability institutions, and eliminating undue influence of money in politics in Australia. Board members of the Centre are the Hon Stephen Charles AO KC, the Hon Anthony Whealy KC, the Hon Pamela Tate KC, Professor George Williams AO, Professor Joo Cheong Tham, Geoffrey Watson SC and Professor Gabrielle Appleby. More information at www.publicintegrity.org.au.