Law Council
OF AUSTRALIA

Office of the President

23 April 2024

Mr Jake Blight
Independent National Security Legislation Monitor
3–5 National Circuit
BARTON ACT 2600

By email: INSLM@inslm.gov.au

Dear Mr Blight

Review of Secrecy Offences in Part 5.6 of the *Criminal Code Act 1995* (Cth)

The Law Council appreciated the opportunity to appear at the public hearing held on Tuesday, 26 March 2024 to assist with your review of secrecy offences in Part 5.6 of the *Criminal Code Act 1995* (Cth). At the hearing, we undertook to provide you with our views about your preliminary recommendations for amending the deemed harm offences relating to inherently harmful information in section 122.1, and the serious harm offences identified by information that causes harm to Australia's interests in section 122.2 of the Criminal Code.

Preliminary recommendation to amend the definition of 'inherently harmful information' and related offences in section 122.1

Your first preliminary recommendation is about the definition of '*inherently harmful information*' contained in section 121.1. That definition is picked up by the offences contained in section 122.1, which prohibit communication and other dealings with inherently harmful information. You have suggested that the current definition be repealed and replaced with a new definition that is confined to: '*information relating to the operations, capabilities or technologies of, or methods or sources used to obtain or disseminate intelligence information*'. You have also suggested that '*intelligence information*' be defined as follows.

- For ASIS, ASD, AGO and DIO, by reference to the existing definition of '*intelligence information*' in the *Intelligence Services Act 2001* (Cth).
- For ASIO it would cover intelligence relevant to '*security*' as defined in the *Australian Security Intelligence Organisation Act 1979* (Cth) (the **ASIO Act**); as well as ASIO's foreign intelligence function in section 17(1)(e) of the ASIO Act.
- For ONI it would cover intelligence relating to section 7(1)(c), (d), (e), (f) and (g) of the *Office of National Intelligence Act 2018* (Cth) (the **ONI Act**).

Telephone +61 2 6246 3788 • *Email* mail@lawcouncil.au
PO Box 5350, Braddon ACT 2612 • Level 1, MODE3, 24 Lonsdale Street, Braddon ACT 2612
Law Council of Australia Limited ABN 85 005 260 622
www.lawcouncil.au

In principle, the Law Council **supports** your recommendation to narrow the scope of the definition of '*inherently harmful information*' for the following reasons.

- As stated in our primary submission, we accept the need for specific secrecy offences that deem any disclosure of precisely defined categories of intelligence information, by intelligence and security officials, as harmful.[1] We accept that there are 'certain paradigm cases' of intelligence-related functions—often relating to the exercise of, and capabilities and technologies relating to, covert powers—that would cause harm if disclosed. For example, disclosing details of secret technology used by ASIO or ASD for lawful electronic surveillance that would allow that surveillance to be avoided.[2]

- We reiterate our view that the onus is on security agencies to establish the necessity and proportionality of the category of intelligence information grounding a deemed harm secrecy offence—having regard to the scope of existing specific offences—contained in the Intelligence Services Act, the ASIO Act, and the ONI Act—that relate to the intelligence agencies.[3] Our concerns regarding the resulting overlap between a reformulated section 122.1 and existing offences that apply to current and former intelligence agency staff and affiliates are set out below.

- We strongly endorse removing the definition of '*security classified information*' from the definition of '*inherently harmful information*'. We consider '*security classified information*' an insufficiently precise term to define the scope of a deemed harm secrecy offence because it is, at least partly, dependent on the content of administrative instruments that are subject to variation from time to time. We consider this to be inconsistent with the rule of law. We have previously recommended that there should be greater specification, on the face of the legislation, of the categories of intelligence information triggering this deemed harm offence.[4]

- For reasons we have set out in our primary submission, we agree that the definition of '*inherently harmful information*' should not separately refer to information that was obtained by, or made by or on behalf of, a foreign intelligence agency.[5]

- We support removing information relating to the operations, capabilities or technologies of, or methods or sources used by, a domestic or foreign law enforcement agency from the scope of the deemed harm secrecy offence.[6]

In line with the Australian Law Reform Commission's views, we consider that the deemed harm offences in a remodelled section 122.1 should only extend to conduct that involves communication. In other words, these specific secrecy offences should not extend to 'conduct other than the disclosure of information—such as making a record of, receiving or possessing information—unless such conduct would cause, or is, likely or intended to cause, harm to an essential public interest.'[7] We do not support retaining inherently harmful information related offences pertaining to conduct other than communication currently in the Criminal Code: sections 122.1(2) (other dealings with inherently harmful information), 122.1(3) (information

[1] Law Council of Australia, Submission to Independent National Security Legislation Monitor, Secrecy Offences in Part 5.6 of the Criminal Code (Submission, 18 March 2024), 18 [36] and Recommendation 1. ('***Law Council's March 2024 Submission***')
[2] Law Council's March 2024 Submission, 22 [55].
[3] Ibid, 24 [64].
[4] Ibid, 18 Recommendation 1.
[5] Ibid, 26 Recommendation 6.
[6] Ibid, 27 Recommendation 7.
[7] Australian Law Reform Commission, Secrecy Laws and Open Government in Australia, Report No 112 (December 2009), 325 Recommendation 9.3. ('***ALRC's 2009 Secrecy Laws Report***')

removed from, or held outside, proper place of custody) and 122.1(4) (failure to comply with direction regarding information).

In our view, the offence in section 122.1 should be distinguished by a narrow framing in respect of the category of intelligence information **and** also the category of person caught by the provision. We have come to this conclusion because even the category of '*information relating to the operations, capabilities or technologies of, or methods or sources used to obtain or disseminate intelligence information*' is likely to capture a range of information including, in some cases, matters that are common knowledge.

As Dr David Neal SC observed at the hearing, in some cases the prima facie assessment by security agencies of what information is connected with operations and capabilities is likely to be over-broad and capture matters that are well known in the community.[8]

We **recommend** that the prosecution be required to prove that, at the time the unauthorised disclosure was made, the '*information relating to the operations, capabilities or technologies of, or methods or sources used to obtain or disseminate intelligence information*' was, applying the ordinary meaning of the word, *secret*.[9] For example, if a Commonwealth employee makes disclosures about the technology underpinning surveillance devices employed by intelligence agencies—where those matters are publicly disclosed by the manufacturer in its advertising for the surveillance product—we do not consider that this disclosure should be proscribed by a deemed harm offence intended to apply to inherently harmful intelligence information.

We are concerned that the application of the mosaic principle—as it has been interpreted by intelligence agencies in their evidence to your inquiry—to the assessment of what information relates to operations, capabilities and methods or sources, is likely to lead to over-inclusive interpretation of this category. In this regard, the ONI provided evidence that:[10]

> *Unauthorised disclosure subjects seemingly innocuous information to 'mosaic analysis'. A foreign intelligence service can use this information together with other available sources (including large data sets and advanced analytical tools) to reveal even more sensitive national security information.*
>
> *All information acquired by, or made by or on behalf of, an intelligence agency in connection with its functions should be considered a source of potential harm if subject to unauthorised disclosure.*

If this approach is taken to be the interpretation of what constitutes information relating to the 'operations, capabilities or technologies of, or methods or sources', it is unclear whether this will be any real improvement from the current situation. We do not agree with using the mosaic principle to over-extend already nebulous, physical elements of the offence provisions. We consider that the mosaic principle should legitimately inform the assessment of the mental state of privileged insiders who are on notice, for example, because of contracts of employment and information security related training, of the implications of disclosure of intelligence information.

---

[8] Independent National Security Legislation Monitor, Transcript of Proceedings—Review of the Secrecy Offences in Part 5.6 of the Criminal Code Act 1995 (Cth) (Day 2, Tuesday 26 March 2024), 164-165 (Dr David Neal SC). ('***INSLM Hearing Day 2 Transcript***').

[9] For completeness, we consider the defence in section 122.5(2) to be too restrictive. Section 122.5(2) provides a defence, subject to an evidential onus on the defendant, where the relevant information has already been communicated or made available to the public *with the authority of the Commonwealth*. We consider that this will be very difficult for a defendant to establish.

[10] Office of National Intelligence, Submission to Independent National Security Legislation Monitor, Review of Secrecy Offences in Part 5.6 of the *Criminal Code Act 1995* (Cth) (Submission, 1 March 2024), 2-3. ('**ONI 2024 Submission**')

To illustrate the potential over-breadth of interpreting information relating to the operations, capabilities, technologies, methods or sources in light of the mosaic principle, we suggest consideration of the following examples:

- An employee of a private firm that is a Commonwealth service provider (within the meaning of 'Commonwealth officer') discloses that AFP officers are unlawfully exceeding the scope of data disruption warrants, which authorise law enforcement agencies to disrupt the transmission of data to, or from, a computer, with a view to frustrating the commission of an offence under the *Surveillance Devices Act 2004* (Cth).

- A Commonwealth employee, who is not a holder of the highest level of security clearance, makes disclosures based on inferences, drawn from publicly available information, including civil society reports commenting on activities of other five-eyes jurisdictions alongside a reading of the ONI Act and publicly available privacy guidelines, about the discriminatory impact of artificial intelligence tools in the context of open-source intelligence activities on certain ethnic minorities.

In both cases, it is conceivable that the actual information disclosed, in isolation, may not contain information pertaining to operations, capabilities or technologies of, or methods or sources. However, it could be argued that, in the aggregate, foreign adversaries would be able to draw damaging inferences about current intelligence and law enforcement capabilities by reference to this information. We consider that criminal liability in both cases should be defined by harm rather than being automatically caught by a deemed harm offence provision.

The Law Council acknowledges that there will be some initial uncertainty about the ambit of any deemed harm secrecy offence. We consider that this arises from the basic problem that harm, being a well-understood term in criminal law, is also more easily capable of determination by a jury. This is again a reason why deemed harm offences must be narrowly confined.

To ensure the consistency of prima facie assessments by agencies of the amended definition of '*inherently harmful information*', we **recommend** that agencies publish guidance on the interpretation of what constitutes information relating to the operations, capabilities or technologies of, or methods or sources used to obtain or disseminate intelligence information by NIC agencies. As indicated in our primary submission, we are most concerned about the potential overbreadth of this phrase in the context of the increasing collection and assessment of open-source information.[11] For example, your proposed definition of 'intelligence information', in the context of the ONI, will capture its functions to '*assemble, correlate and analyse information relating to other matters that are of political, strategic or economic significance to Australia*'.[12] We have previously explained that economic significance is liable to capture a range of transactions that are remote from inherent damage to national security interests.[13]

We disagree with your preliminary view that the offence provisions in section 122.1 should continue to apply to all '*Commonwealth officers*'. That approach would extend to an individual who is a contracted service provider for a Commonwealth contract and employees of a contracted service provider for a Commonwealth contract.[14] We adopt this view for the following reasons.

[11] Law Council's March 2024 Submission, 22 [57].
[12] ONI Act, s. 7(1)(d)(i).
[13] Law Council's March 2024 Submission, 32 [98] – [100].
[14] Within the meaning of Criminal Code, section 121.1 ('*Commonwealth Officer*').

We note that definitions of intelligence and security officials, in the context of existing specific secrecy offences, already have the capacity to capture a wide range of persons because they apply to former, as well as current, officials, and contractors.

- Generally, existing specific secrecy offences apply to current and former employees of relevant intelligence agencies. For example, the offence in section 39 of the Intelligence Services Act proscribes disclosure of information that has come to the knowledge of a person by reason of them being, or having been, a staff member or agent of ASIS.

- The current scope of specific offences regulating intelligence officials has the capacity to regulate a wide range of persons including contractors. For example, the definition of '*ASIO Affiliate*' in the ASIO Act means 'a person performing functions or services for the Organisation in accordance with a contract, agreement or other arrangement' and includes consultants and contractors engaged on behalf of the Commonwealth by written agreement (under section 85 of the ASIO Act). Similarly, the offences in the Intelligence Services Act proscribe disclosures where the information has come to the knowledge of a person by reason of his or her having been an employee or agent of a person who has entered into a contract, agreement, or arrangement with the relevant NIC agency.[15]

We consider that extending the scope of an exceptional deemed harm specific secrecy offence to '*Commonwealth officers*' would undercut the overarching principle that general secrecy offences should require proof of actual harm. Again, we reiterate our support for the development and amendment of Commonwealth secrecy provisions in a manner consistent with the Australian Law Reform Commission's 2009 report: *Secrecy Laws and Open Government in Australia*. The ALRC underlined the need to confine a deemed harm offence, based on the inherent sensitivity of intelligence information, to current and former intelligence staff and those who work with them noting:[16]

> *The ALRC considers that a prohibition on the disclosure of information obtained or generated by intelligence agencies is justified by the sensitive nature of the information and the special duties and responsibilities of officers and others who work in and with such agencies. The existing (Australian Intelligence Community) secrecy offences cover a limited range of people who handle intelligence information, namely officers and employees, and people with whom the agency has an agreement or arrangement. The ALRC considers that it is appropriate for people in this position to be subject to higher responsibilities to protect inherently sensitive intelligence information.*

Currently, by way of mental element, section 122.1 only requires that a person is reckless that the information is '*inherently harmful information*'. For the reasons explained in our primary submission, this represents an extraordinarily low threshold.[17] Instead, we have suggested greater differentiation in identification of the culpability of Commonwealth officers who make unauthorised disclosures.[18] If there is to be a deemed harm offence that applies to all Commonwealth officials requiring only recklessness with respect to the category of information, it should only be framed as a summary offence as we have suggested in our primary submission.[19]

As we have previously argued, paragraph 3 of Article 19 of the *International Covenant on Civil and Political Rights*[20] requires, relevantly, that restrictions on the right to freedom of expression must relate to the protection of national security, be 'provided by law', and must conform to

[15] See for example, *Intelligence Services Act 2001* (Cth), s. 39 (Communication of ASIS information).
[16] ALRC's 2009 Secrecy Laws Report, 289 [8.62].
[17] Law Council's March 2024 Submission, 27 [74] – [75].
[18] Law Council's March 2024 Submission, 28 Recommendation 8.
[19] Ibid.
[20] opened for signature 19 December 1996, 999 UNTS 171 (entered into force 23 March 1976).

'strict tests of necessity and proportionality'. We consider that lack of differentiation in the class of persons targeted by a deemed harm offence increases the risk it will be a disproportionate interference with the right to freedom of expression because, as noted by United Nations Human Rights Committee, 'restrictions must be applied only for those purposes for which they were prescribed and must be directly related to the specific need on which they are predicated'.[21] It is not proportionate to extend an exceptional deemed harm offence to all Commonwealth officials (and contractors and their employees) because a narrow class of that cohort (for example, senior staff members of the Department of the Prime Minister and Cabinet or the Attorney-General's Department) may come across the prescribed type of intelligence information.

For the reasons outlined above, we **recommend** that a new definition of '*intelligence official*' and '*intelligence affiliate*' be inserted into the Criminal Code. For example, '*intelligence official*' should include, by reference to the ambit of current offences in the Intelligence Services Act, current and former 'staff members' or employees of intelligence agencies as well as 'those with a contract, agreement or arrangement' with an NIC agency. We accept that there may be a need, given the 'importance of protecting sensitive intelligence sources and methods', for these offences to extend to 'those who may assist agencies in other ways which are not consistent with a relationship of employment or contract service provision'.[22]

In the alternative, we **recommend** that the offences contained in section 122.1, which prohibit communication and other dealings with inherently harmful information, should only apply to the most sensitive class of users of national security classified information: that is, the holders of the highest level of security clearance. We note that the Department of Home Affairs has provided evidence that 'these individuals can be identified as a class through their holding of the Commonwealth's highest level of security clearance'.[23] Our submissions are intended to illustrate the availability of more proportionate alternatives to making the deemed harm offences contained in section 122.1 relating to inherently harmful information apply to all '*Commonwealth officers*'.

Finally, we **recommend**, in line with the ALRC's views, that the remodelled offences contained in section 122.1 should require that the intelligence official or affiliate knew, or was reckless as to whether, the protected information fell within the category of 'inherently harmful information'.[24] In other words, the offence should not provide that strict liability applies to that circumstance element.

[21] United Nations Human Rights Committee, General Comment 34: Article 19: Freedoms of Opinion and Expression, 102nd sess, Un Doc CCPR/C/GC/34 (12 September 2011), 6 [22].
[22] Office of National Intelligence, Submission to Independent National Security Legislation Monitor, Review of Secrecy Offences in Part 5.6 of the *Criminal Code Act 1995* (Cth) (Submission, 1 March 2024). ('**ONI 2024 Submission**')
[23] Department of Home Affairs, Submission to Independent National Security Legislation Monitor, Review of the Secrecy Provisions Contained within Part 5.6 of the Criminal Code At 1995 (Cth) (March 2024), 7.
[24] ALRC's 2009 Secrecy Laws Report, 334 Recommendation 9.6.

Repeal of specific secrecy offences contained in the *Intelligence Services Act 2001* (Cth), the *Australian Security Intelligence Organisation Act 1979* (Cth), and the *Office of National Intelligence Act 2018* (Cth)

We **recommend**—after the definition of 'inherently harmful information' and related offences in section 122.1 is restricted in the manner discussed above—existing specific secrecy offences contained in the Intelligence Services Act, the ASIO Act, and the ONI Act should be repealed. Then, reliance should be placed on the reformed offences in the Criminal Code in respect of regulating disclosures by all NIC agency officials and affiliates. As a general principle, we agree with the Guide to Framing Commonwealth Offences[25] that offences of general application should be set out in the Criminal Code rather than creating new offences. As the Guide notes:[26]

> *Broadly framed provisions of general application were placed in the Criminal Code to avoid the technical distinctions, loopholes, additional prosecution difficulty and appearance of incoherence associated with having numerous slightly different provisions of similar effect across Commonwealth law.*

If our recommendation is not accepted, we are concerned that this will lead to arbitrary differentiation resulting from the prosecutor's discretionary decision to press charges in relation to 'inherently harmful information' and related offences in section 122.1 rather than intelligence-related specific secrecy offences.

First, the different thresholds (between a more proportionate and targeted definition of 'inherently harmful information' and related offences in section 122.1, and the very broad specific secrecy offences contained in the Intelligence Services Act, the ASIO Act, and the ONI Act, applicable defences and penalties) may result in inconsistent treatment of similar cases. We consider it to be a critical facet of the rule of law, as well as the administration of justice, that like cases should be treated alike and that the law should not discriminate between people on arbitrary or irrational grounds.[27] The potential for inconsistent treatment is illustrated by reference to examples below.

- A contractor who provides services to ASD will be subject to the exceptionally broad offences contained in sections 40, 40G and 40H of the Intelligence Services Act. Section 40 prohibits disclosure of any information or matter that was acquired or prepared by or on behalf of ASD in connection with its functions or relates to the performance by ASD of its functions and is punishable by imprisonment for 10 years. Each offence is only subject to very limited exceptions—most notably, that the offence does not apply to information or matter that has already been communicated or made available to the public with the authority of the Commonwealth. None of these offences contains the wider range of defences contained in section 122.5. For example, the offence in section 40 is not subject to a defence for communication of information for the purpose of obtaining legal advice in relation to a Part 5.6 offence as contained in section 122.5. An ONI employee would only be permitted to make such a disclosure, within the course of their duties, or with the approval of the relevant Director-General, for example, as provided under section 42(1)(c)(iv) of the ONI Act.[28]

[25] Attorney-General's Department, A Guide to Framing Commonwealth Offences, infringement Notices and Enforcement Powers, 2011.
[26] Ibid, 14.
[27] Law Council of Australia, Policy Statement—Rule of Law Principles (March 2011), Principle 2.
[28] The Law Council notes ONI evidence in their 2024 Submission, 13: '[s]uch approvals are routinely provided, but in some cases agencies may prefer to use cleared lawyers, experienced in handling classified material and with access to more robust ICT systems. Agencies may also decline to approve, or provide reasonable caveats to such approvals.'

- A contractor who provides services to the Commonwealth who discloses similar information, for example, pertaining to the operations, capabilities or technologies of the intelligence functions of ASD as defined by the Intelligence Services Act would be treated more favourably under a prosecution of the remodelled the offences contained in section 122.1. For example, if the definition of 'inherently harmful information' is narrowed in the way you suggest, it will be substantially narrower than the framing of section 40 of the Intelligence Services Act. Communication of inherently harmful information under section 122.1(1) is subject to the maximum penalty of imprisonment for 7 years. In this case, the wider range of defences contained in section 122.5 are available (for example, information communicated for the purpose of reporting offences and maladministration and in relation to legal advice).

We disagree with the ONI's view that the current specific secrecy offences in the ONI Act should be retained because of the absence of exceptions that are contained in the Criminal Code.[29] We consider the presence of exceptions critical to maintaining the proportionality of deemed harm offences.

Other practical matters

We are concerned that the intent of your preliminary recommendation—in restricting the scope of '*inherently harmful information*'—may be frustrated by certain practical constraints. As noted by Mr Phillip Boulten SC, in his evidence before you, classification decisions are an unsatisfactory parameter of criminal offence because of limitations on: '…how that gets analysed, who analyses it, who makes the decisions, whether or not there's any auditing, whether or not there's slippage, whether there's an objective way for an outsider to get access to the decision making process'.[30] We consider that similar concerns apply to the prima facie assessment by an official regarding whether the disclosure contains '*information relating to the operations, capabilities or technologies of, or methods or sources used to obtain or disseminate intelligence information*' by NIC agencies. In this regard, we suggest consideration of the following matters.

The constraints that may be imposed on an individual prosecuted under section 122.1, and their defence counsel, to contest the prima facie assessment that information is appropriately classified as '*information relating to the operations, capabilities or technologies of, or methods or sources used to obtain or disseminate intelligence information*' by NIC agencies, include the following matters.

- In this regard, it is likely that prosecutions under section 122.1 will be subject to interoperation with the *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth) (**NSI Act**). That interoperation could relate to the aspects of the NSI Act that fetter the Court's ability to deal with certain information in its usual way—departing from the principle of open justice as well as the accused's right to a fair trial. This carries the risk of disproportionate interference with the affected individual's right to a fair trial and fair process rights.

- Members of the Law Council's National Criminal Law Committee express reservations about the over-extensive approach taken by the Commonwealth to asserting public interest immunity, including in matters where the NSI Act has already been invoked. This often has the effect that defence counsel is granted access to certain information but only after significant expense and delay.

[29] ONI 2024 Submission, 10-11.
[30] INSLM Hearing Day 2 Transcript, 161.

- Further to the above, we underline the importance of compliance with the prosecutor's ethical duty of disclosure (noting that this may be practically dependent on cooperation with other government agencies), as set out in the CDPP's Statement on Disclosure, which is critical to the administration of justice and the court's ability to ensure a fair trial. We are troubled by recent examples in national security related prosecutions where disclosure has been found to be insufficient.[31]

To address these matters, we reiterate our **recommendation** that the recommendations of the fourth Independent National Security Legislation Monitor, Grant Donaldson SC in his report into the operation and effectiveness of the NSI Act should be implemented.[32] In this regard, we have highlighted the importance of the recommendations directed to new obligations on the Attorney-General to conduct regular reviews of material that has been kept secret by reason of the NSI Act, to determine if secrecy is no longer required; and restoring principled discretion by judges, rather than the potentially inflexible operation of mandatory directions in the NSI Act, about how courts are to deal with and decide certain matters.

We note that, in your questions of intelligence and security agencies, you asked for further information regarding parameters for independent verification and review of classification decisions under the PSPF by agencies. To provide greater independent verification of the prima facie assessment by officials whether information relates to the operations, capabilities or technologies of, or methods or sources used to obtain or disseminate intelligence information by NIC agencies, we **recommend** that there be publicly available guidance documents that identify best practice for independent audit and review processes.

Preliminary recommendation to amend the definition of 'causes harm to Australia's interests' and related offences in section 122.2

You propose recommending that amendment of the definition of '*cause harm to Australia's interests*' in section 122.1 to be repealed and replaced to mean:

- prejudice security, defence or international relations;
- impede the prevention, detection, investigation or prosecution of crime by a law enforcement agency;
- impede the performance of the functions of the Australian Federal Police under:
    - Paragraph 8(1)(be) of the *Australian Federal Police Act 1979* (Cth) (protective and custodial functions); or
    - the *Proceeds of Crime Act 2002* (Cth);
- cause harm to the health or safety of the Australian public or a section of the Australian public.

We note that your preliminary recommendation to include AFP protective and custodial functions is contingent on those functions being described in a publicly available legislative instrument as required by section 8A of the AFP Act. We would be grateful to review a copy of this legislative instrument in order to provide a view on this matter.

[31] See further, Fourth Independent National Security Legislation Monitor, Grant Donaldson SC, Annual Report (Annual Report, 2022-2023) 13 [39] – [40] (non-disclosure of Dr Emily Corner's report raising doubts about the methodological rigour of the risk assessment tool employed in relation to Division 105A of the Criminal Code).
[32] Law Council of Australia, 'National Security Information Act must have sufficient regard to open justice' (Media Release, 4 December 2023).

We **support** the amendments, indicated above in red, which are directed to providing greater specification of materiality thresholds. This is consistent with recommendations we made in our submission.[33]

We **support** your proposal that 'security' would be defined consistently with the ASIO Act, which is consistent with our recommendation.[34]

We **support** your proposed modifications to the definition of 'defence' in line with Mr Donaldson's recommendations in his NSI Act Report, which are consistent with our recommendation.[35]

We welcome your proposal to restrict the definition of 'international relations', by removing economic relations from the definition.[36] However, we consider the inclusion of 'bilateral and multilateral, police and intelligence cooperation arrangements' is uncertain and overinclusive. Because an increasing number of Commonwealth offences carry a transnational element, and there is an increasing trend towards international cooperation in regulating these risks, these types of police arrangements can cover a very wide range of matters.

We submit that there is an important difference between the national security interests at stake in the continuation of bilateral and multilateral arrangements for intelligence cooperation (for example, the importance of the five-eyes alliance) and the more diffuse benefits of the continuation of international law enforcement arrangements pertaining to the enforcement of criminal offences more generally. In our view, only the former warrants protection in the context of a deemed harm secrecy offence. Accordingly, we do not support inserting 'bilateral and multilateral, police and intelligence cooperation arrangements' in the definition of 'international relations'.

We **support** incorporating a definition of 'law enforcement agency' to provide greater certainty. However, we are not persuaded that it is necessary to include AUSTRAC in that definition.

For reasons we have previously set out, we reiterate our **recommendation** that the definition of '*cause harm to Australia's interests*' should not be extended to disclosures that impede the functions of the Australian Federal Police under the *Proceeds of Crime Act 2002* (Cth).[37] We remain of the view that it is unduly harsh to impose criminal sanctions, in the general secrecy offence, for disclosures of information that threaten civil or administrative processes, such as the proceeds of crime regime.

Alternatively, we **recommend** that the differentiation in objective seriousness between disclosures that cause harm to law enforcement interests (which is most pressing in the context of imminent threats to the safety of members of the public and less urgent in the context of enforcement of an administrative process) compared to prejudice to 'security', 'defence' or 'international relations' would be more accurately captured by separating law enforcement related matters into a new summary offence with a lower penalty.

[33] Law Council's March 2024 Submission, 30 Recommendation 10.
[34] Ibid, 34-35 Recommendation 15.
[35] Ibid.
[36] Ibid, 32 – 33 Recommendation 13.
[37] Law Council's March 2024 Submission, 31-32 Recommendation 12.

In this regard, the ALRC observed:[38]

> *Because of the breadth of information obtained or generated by police services, the seriousness of the harm caused by the unauthorised disclosure of information in law enforcement agencies may range from negligible to severe, depending on the nature of the information and the timing and context of the disclosure.*

Final matters

We **recommend** that the Inspector General of Intelligence Services conduct an updated review evaluating implementation of its Preliminary Inquiry into the application of national security classifications in ASIO, ASIS, ONI, ASD, AGO and DIO dated 25 February 2021[39]— in particular, the adequacy of measures taken since 2021 to enhance the currency and awareness of written guidance on national security classifications, and the suitability and frequency of training in the application of national security classifications.

Contact

If you require further information or clarification, please contact [redacted]

Yours sincerely

Greg McIntyre SC
President

[38] ALRC's 2009 Secrecy Laws Report, 292 [8.77].
[39] Inspector General of Intelligence and Security, the Hon Christopher Jessup KC, Preliminary Inquiry into the application of national security classifications in ASIO, ASIS, ONI, ASD, AGO and DIO (Preliminary Inquiry Report, 25 February 2021).