Secrecy Bill – OVERVIEW OF KEY ISSUES AND ARTK CONCERNS

ISSUES		ARTK POSITION (IF ANY)	AGD REVIEW (21 NOVEMBER 2023)	INSLM REVIEW (27 JUNE 2024)	GOVERNMENT RESPONSE TO INSLM REVIEW (27 NOVEMBER 2024)	SECRECY BILL (2026)
Criminal Code s 122.1(1),(2) — Insider offences for communication or dealing with *"inherently harmful information"*	**Narrow the definition of "*inherently harmful information*"**	The definition of "*inherently harmful information*" **is too broad**: • **Security markings:** Presence of security markings should not dictate whether information is "*inherently harmful information*". This makes a critical element of an offence dependent on the actions of government, contrary to the rule of law. Using a security marking means the offence is not targeted to cases of actual harm as the classification may be outdated or insufficiently directed to genuine national security risks. • **Domestic / foreign intelligence agencies:** Not all information that was "*obtained by, or made on behalf of, a domestic intelligence agency or a foreign intelligence agency in connection with the agency's functions*" should be "*inherently harmful information*", only information which damages their functions if disclosed; • **Law enforcement**: Not all information "*relating to the operations, capabilities or technologies of, or methods or sources used by, a domestic or foreign law enforcement agency*" should be covered. Only information which damages these activities if disclosed should be covered.	AGD does not agree with narrowing the definition, but recommends the INSLM consider this issue.	The definition of "*inherently harmful material*" **is too broad**: • **Security markings:** Presence of security markings should not dictate whether information is "*inherently harmful material*" (INSLM Rec 1). • **Domestic / foreign intelligence agencies:** The concept of "*inherently harmful information*" should be limited to "*intelligence information*" and the operations, capabilities, technologies, methods, and sources used to obtain or communicate that information (INSLM Rec 2). • If the existing deemed harm category is to remain (i.e. information must relate to the "*functions*" of an intelligence agency), then the functions of the Defence Intelligence Organisation (**DIO**), which currently has no statutory functions, must be set out in legislation or disallowable legislative instrument so that Parliament controls the scope of the offence (INSLM Rec 5). • **Law enforcement**: The concept of "*inherently harmful information*" should be limited to **i**nformation that relates to the technologies, capabilities and methods used to exercise special electronic surveillance powers (INSLM Rec 3).	Agreed that the definition of "*inherently harmful material*" is too broad: • **Security markings**: agreed with INSLM Rec 1 that the offences in Part 5.6 should not rely on information being security classified as an element of the offence and agreed to repeal the security classified information limbs of the deemed harm offences in s 122.1 and the outsider offence in s 122.4A. • Said it would consider whether explicitly providing that the presence of security classification markings is relevant to proving fault elements in these offences. • **Domestic / foreign intelligence agencies: Government** noted INSLM's Rec 2 that the deemed harm offences in s 122.1 should not apply to all information connected to an intelligence agency's functions and committed to assess the feasibility of legislating a narrower definition. • Committed to require the publication of the functions of DIO (Government Response, p 4). • **Law enforcement:** agreed in principle to INSLM Rec 3 that the deemed harm offences in s 122.1 should not apply to all information used by a domestic or foreign law enforcement agency. Agreed to confine the categories of law enforcement information to information in which there is an essential public interest that needs to be protected by criminal sanctions.	ARTK concerns not addressed, save for removal of security markings: • **Security markings**: while the Bill repeals the security marking limbs of the deemed harm offences in s 122.1 and the outsider offence in s 122.4A, the EM includes a range of legally incorrect statements that attempt to equate the existence of a security marking as definitive evidence of whether a defendant has satisfied relevant fault elements of these offences (EM [307] – [310]; [257] – [261]). This is an attempt to reinstate security classifications as a defacto element of the offence and must be removed. • **Domestic / foreign intelligence agencies:** no amendments made despite Government committing to assess "*feasibility*" of an narrower definition. • The Bill requires publication of the document known as the "*Defence Intelligence Mandate*" (Sched 4 item 46). DIO's functions do not need to be set out in that document and Parliament still does not set the parameters of the DIO's functions (and through that the scope of the offence) under this amendment. • **Law enforcement:** no amendments made despite agreement in principle to narrow this category.
	Change fault elements from recklessness to intention	All harm based elements of these offences set out in the definition of "*inherently harmful information"* should use as a mental element intention rather than recklessness. e.g. rather than the defendant been liable if they are aware of a "*substantial risk*" that information "*relating to the operations, capabilities or technologies of, or methods or sources used by, a domestic or foreign law enforcement agency*" and proceeding without justification (the recklessness standard), the defendant should only be liable where they believe this circumstance exists or will exist (the intention standard).	AGD considered that current recklessness fault element is appropriate.	On balance, **the recklessness element should remain**. However there are "*strong arguments*" to use an intention rather than recklessness element in the *outsider offence* in s 122.4A .	Not dealt with.	ARTK concerns not addressed.
	Clarify concept of dealing to remove passive receipt of information	For offences that apply where a defendant "*deals*" with information, the current definition in s121.1 (which refers back to the definitions in s 90.1(1) and (2) is **too broad** and potentially captures the unsolicited receipt of information.	AGD considers unsolicited receipt or other unwitting dealings will not be sufficient to reach the threshold of intention required by ss 122.1(2), 122.2(2) and 122.4A(2).	The definition of "*deals*" should be **clarified and narrowed**: • Receiving information should be removed from the definition of "*deals*" (INSLM Rec 7). • Various other minor clarifications to the definition were recommended.	Agreed in principle to INSLM's recommendation that the definition of "*deal with*" be amended.	The Bill *attempts* to address ARTK's concern but fails to do so effectively. The proposed new definition of "*deals with*" uses the concept of "*possesses*" information. But a person "*possesses*" information when it is in their possession regardless of how it came there. Passive receipt is therefore still potentially covered (Bill Sched 4 Item 5).

ISSUES		ARTK POSITION (IF ANY)	AGD REVIEW (21 NOVEMBER 2023)	INSLM REVIEW (27 JUNE 2024)	GOVERNMENT RESPONSE TO INSLM REVIEW (27 NOVEMBER 2024)	SECRECY BILL (2026)
Criminal Code ss 122.2(1),(2) – Insider offences for conduct *"causing harm to Australia's interests"*	**Narrow the definition of *"causing harm to Australia's interests"***	The definition of "*causing harm*" is **too broad** and should be narrowed: • **Security or defence of Australia:** "*Causing harm*" currently incorporates the definition of "*security or defence of Australia*". This definition is currently unacceptably broad and uncertain and includes deeming elements that have nothing to do with the security or defence of Australia – e.g. "*the operations, capabilities or technologies, or methods or sources used by, domestic or foreign intelligence agencies*". • ARTK otherwise broadly accepts the changes to the definition of "*causing harm*" proposed by the INSLM relating to **international relations** and **law enforcement** and the applicable materiality thresholds for harm to these interests – see column 4.	The AGD does not agree with narrowing the definition of "*causing harm*" to Australia's interests.	The definition of "*causing harm*" **should be narrowed**: • **Materiality threshold**: The materiality threshold for each category used in the definition of "*causing harm*" must be material harm being caused by the disclosure or the likelihood of material harm. • **Security or defence of Australia**: this limb should be narrowed, with "*security*" defined as per the ASIO Act and "*defence*" defined based on the definition used in the UK Official Secrets Act. • **International relations**: this limb should be narrowed, with "*international relations*" defined to cover diplomatic and military relations and international law enforcement and intelligence cooperation arrangements. • **Law enforcement**: this limb should be narrowed to cases of harm or likely harm to the utility of capabilities connected to statutory powers to access information or search people/places/things to combat crime; and harm or likely harm to AFP protective, custodial and proceeds of crime functions. • **Health and safety**: this limb should be limited to cases of harm or likely harm to health or safety of the Australian public (this recommendation is substance reflects the current offence – no amendments needed). (INSLM Rec 6).	**Agreed to narrow** the definition of "*causing harm*" as follows: • **Materiality threshold:** The Government response did not expressly adopt the INSLM's specific recommendation on materiality thresholds, but appears implicitly to accept them. • **Security or defence of Australia:** Agreed to implement INSLM rec on definition of "*security*". Will consider definition of "*defence*" in context of defence reforms; • **International relations**: Government does not agree to INSLM recommendation to narrow current definition to exclude economic relations. • **Law enforcement**: Government does not agree to any changes to current law enforcement related definition.	ARTK concerns not addressed: • **Materiality threshold**: The INSLM recommended a threshold that required material harm or the likelihood of material harm. The proposed amendments to the materiality threshold (Sched 4 items 1-4) do not appear to make any substantive difference to the operation of the existing definitions. The amendments remove references to "*harm*" but retaining references to "*prejudice*" to the relevant interests (e.g. defence), which does not achieve what the INSLM sought. • The discussion of "*prejudice*" in the EM is inappropriate because "*prejudice*" is not statutory language introduced by the Bill. Nor does the EM's discussion appear to align with the INSLM's recommendations for a material harm standard. • **Security or defence of Australia:** although an attempt to implement the INSLM's recommendation, the proposed amendments simply incorporate by reference the ASIO Act definition rather than providing clearly in the Criminal Code the new definition of "*security*". This creates a risk of inadvertent changes to the scope of the offence from amendments to the ASIO Act. The definition should be set out in the Criminal Code. • ASIO Act definition of "*security*" is unclear in how it incorporates the security interests of foreign countries. • **International relations** and **Law enforcement:** INSLM recommendations have been ignored. No clear reasons have been given.
	Change fault elements	See row 2 above.	See row 2 above.	See row 2 above.	See row 2 above.	ARTK concern not addressed – see row 2 above.
	Clarify concept of dealing to remove passive receipt of information	See row 3 above.	See row 3 above.	See row 3 above.	See row 3 above.	ARTK concern not effectively addressed – see row 3 above.
Criminal Code ss 122.1(1),(2); 122.2(1),(2) – Insider offences generally	**ABC/SBS staff and contractors should not be covered by the insider offences**	The insider offences apply to ABC and SBS staff and contractors because of a drafting error or the failure to make appropriate regulations. They should not be subject to these offences.	Not dealt with.	ABC/SBS staff and contractors should not be covered by the offences for officials.	Seemingly agreed in principle.	ARTK concerns addressed in substance – however the relevant amendments should be backdated to the commencement of these offences as it was never the intention to apply these offences to ABC and SBC staff and contractors.
Criminal Code 122.3 – Aggravated insider offences involving dealings with *"inherently harmful information"* or *"causing harm to Australia's interests"*	**Circumstances of aggravation for government officials should be narrowed**	These amendments do not directly impact journalists but may impact journalist sources. ARTK does not express a position.	Not dealt with.	The maximum penalty for offences by 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 • The person intended or knew their conduct would or was likely to cause a type of harm covered by the underlying offence.	Agreed.	ARTK does not express a position.

ISSUES		ARTK POSITION (IF ANY)	AGD REVIEW (21 NOVEMBER 2023)	INSLM REVIEW (27 JUNE 2024)	GOVERNMENT RESPONSE TO INSLM REVIEW (27 NOVEMBER 2024)	SECRECY BILL (2026)
Criminal Code ss 122.1(3), 122.2(3) – removing certain information from its "*proper place of custody*"	**The offence should be repealed**	These offences **should be repealed**. The regulations required to make them function have never been made.	AGD **recommended the repeal** of the proper place of custody offences (AGD Rec 6).	The "*proper place of custody*" offences **should be repealed**, as relevant regulations to define 'proper place of custody' have never been made in the nearly 6 years since enactment, indicating they are not necessary. The conduct is already covered by 'dealing with' offences. (INSLM Rec 9)	Agreed.	ARTK concern addressed.
Criminal Code s 122.4 – Insider offence of disclosing information subject to a "*duty not to disclose*" imposed by other Commonwealth laws	**The offence should be allowed to sunset**	This offence was a transitional measure designed to allow the identification of any specific statutory non-disclosure duties which may require criminal penalties being attached to them. The period allocated for this task was 5 years and has been since extended to 7. The current s 122.4 offence is **impermissibly broad**, covering information where no meaningful risk to a public interest of sufficient importance to warrant criminal sanction exists.	Section 122.4 should be **repealed or allowed to sunset** (AGD Rec 5).	Clear implication is that the INSLM **agrees with repeal** or allowing the provision to sunset (see INSLM [7.8] onward).	Response **assumes the repeal** or sunsetting of s 122.4.	ARTK concern addressed in substance as the offence will now sunset – however the sunset date is proposed to be extended <u>yet again</u> to 29 December 2026 under the related Secrecy Provisions Amendment (Sunsetting Provision) Bill 2026.
Criminal Code s 122.4 – <u>New</u> Insider offence of *"improper"* dealing with information intended to cause "*benefit*" or "*detriment*"	**The new general secrecy offence should not be introduced**	The new offence: • Is not needed – no clear additional categories of harmful disclosures have been identified that warrant criminal protection through a new secrecy offence. • Is fundamentally indeterminate and so offends the rule of law. • Impermissibly burdens constitutionally protected political communication because it goes far beyond protecting the legitimate public interests that may be protected either by secrecy laws or by misfeasance in public office offences.	The AGD recommends (AGD Rec 3): • **Harms based offence:** The creation of a new harms based general secrecy offence for inclusion in Part 5.6. • That this new harms based offence should, subject to further development, ensure that Commonwealth officers and persons who perform services for or on behalf of the Commonwealth do not make disclosures **prejudicial to the effective working of Government** or where the information was **communicated to them in confidence.**	Any general offence to replace s 122.4 should be consistent with the following principles: • **Harms based offence**: the new offence should be harm-based and relate to essential public interests (any deemed harm offence should be limited to a very narrow category of information where significant harm to essential public interest is always/almost always going to be the result); • The new offence should apply to disclosures that prejudice the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth (i.e. this issue should be taken out of the more serious disclosure offences and placed in the new s 122.4 instead). • The new offence should only cover disclosures that cannot be dealt with by existing remedies. • The penalty for reckless conduct should be no more than 2 years imprisonment . • **Clear framing of offence**: the new offence should avoid broad and uncertain language (e.g. "*prejudicial to the effective workings of government*"). • **Clear confinement of offence to government**: the new offence should apply to current and former Commonwealth officials, and others who perform work for a Commonwealth entity – however, if the scope is to be broadened, it should still be closely linked to some kind of contract/agreement with the Commonwealth. (INSLM Rec 11).	Agreed in part with INSLM's recommendation; • **Harms based offence:** Government agreed that the new offence "*would be consistent with the recommended principles".* • Government did not agree that disclosures that prejudice the prevention, detection, investigation, prosecution or punishment of a Commonwealth criminal offence should be covered by the new offence. They should instead continue to be covered by the more serious offence in s 122.2.	ARTK concerns not addressed: • **Harms based offence: n**o explanation has been given for why the harms based approach recommended by the AGD, the INSLM and agreed to by Government has now been rejected. Rejecting a harms based approach creates significant constitutional and policy problems. • **Clear framing of offence**: the INSLM specifically recommended the need for clear language in criminal offences. No explanation has been given for why the offence is now even more indeterminate then the proposals considered by the INSLM – particularly through its key concepts of "*improper*" use of information with an intention to "*benefit*" or cause "*detriment*". • The EM contemplates that the new offence will apply whenever a confidentiality duty applies (EM at [26]). This is not a correct. On its true construction, the "*improper*" requirement invites a weighing of reasons for and against disclosing information. But if the EM was correct, this is in impermissible attempt to reinstate the <u>sunsetting version</u> of s 122.4 which criminalizes breach of all current statutory confidentiality duties. • **Clear confinement of offence to government**: it is unclear whether it is appropriate to impose this new form of criminal liability on the very large number of service providers who will now be covered. No consultation appears to have been undertaken so the views of those impacted by the Bill (including APS employees) is unknown. Broader consultation including with civil society was specifically recommended by the

ISSUES		ARTK POSITION (IF ANY)	AGD REVIEW (21 NOVEMBER 2023)	INSLM REVIEW (27 JUNE 2024)	GOVERNMENT RESPONSE TO INSLM REVIEW (27 NOVEMBER 2024)	SECRECY BILL (2026)
						INSLM (INSLM [7.64]). It is unclear why a regulatory impact statement outlining consultations undertaken and broader impacts was not prepared and included in the EM.
Criminal Code s 122.4A — Offence for communications and dealings with certain information by non-Commonwealth officers	**Remove security markings as an element of the outsider offence**	Presence of security markings of Secret or Top Secret should not dictate whether information is covered by this offence. Using a security marking to distinguish information covered by the offence makes a critical element of an offence dependent on actions of government, contrary to the rule of law. Using a marking means the offence is not targeted to cases of actual harm as the classification may be outdated or insufficiently directed to genuine national security risks.	Not dealt with.	The offences in Part 5.6 including s 122.4A should not rely on information being classified under a policy framework as an element of the offence (INSLM Rec 1).	Agreed that the offences in Part 5.6 should not rely on information being security classified as an element of the offence: • Agreed to repeal the security classified information limbs of the deemed harm offences in s 122.1 and the outsider offence in s 122.4A. • Stated that government will consider whether explicitly providing that the presence of security classification markings is relevant to proving fault elements in s 122.1 and 122.4A.	ARTK concerns addressed in substance: • The Bill repeals the security marking limbs of the deemed harm offences in s 122.1 and the outsider offence in s 122.4A (Bill Sched 4 items 6,9, 10, 22) • However, the EM includes a range of legally incorrect statements that attempt to equate the existence of a security marking as definitive evidence of whether a defendant has satisfied relevant fault elements of these offences (EM [307] – [310]; [257] – [261]). This is an attempt to reinstate security classifications as a defacto element of the offence and must be removed.
	Materiality threshold should be increased– the outsider offence should be limited to causing <u>serious harm</u> to a small number of clearly defined public interests	ARTK generally supports the INSLM's recommendations for narrowing these offences.	AGD considered no changes to outsider offences required.	Significant narrowing of these offences is required: • **Materiality threshold**: the current threshold of requiring "*damage*" etc to various listed interests should generally be lifted to require "*serious*" damage etc. The harm threshold should be higher than for officials covered by equivalent insider offences. • **Defence and national security**: this limb should be narrowed to causing serious damage to security/defence of Australia. "*Security*" should be defined as per the ASIO Act and "*defence*" defined based on the definition used in the UK Official Secrets Act (see also INSLM Rec 6). • **Criminal investigations**: the offence currently applies where the "*communication of information interferes with or prejudices the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth*." This should be narrowed and split into two limbs: "*<u>seriously undermining</u> the utility of the technologies, capabilities and methods used to exercise special statutory powers*" and "*<u>seriously impeding</u> the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth*." • **Health and safety of Australian public**: the current limb requiring information harm or prejudice the health or safety of the Australian public or a section of the Australian public should be retained. (INSLM Rec 12).	Agreed in principle with INSLM Rec 12: • **Defence and national security**: Offence should apply to serious harm to "*security*" as defined per INSLM recommendation and "*defence*". A new definition of "*defence*" to be considered in context of reforms to defence legislation. • **Criminal investigations:** Government does not support changes. No clear reasons given.	ARTK concerns not addressed: • **Defence and national security**: although an attempt to implement the INSLM's recommendation, the proposed amendments simply incorporate by reference the ASIO Act definition rather than providing clearly in the Criminal Code what the new definition of "*security*" is. This creates a risk of inadvertent changes to the scope of the offence from amendments to the ASIO Act. The definition should be set out in the Criminal Code. • ASIO Act definition of "*security*" is unclear in how it incorporates the security interests of foreign countries. • The Bill introduces a <u>completely new category</u> of criminalised disclosures <u>that was not recommended by the INSLM</u>: being "*information [that] causes serious damage to the operations, capabilities or technologies of, or methods or source used by, a domestic intelligence agency or foreign intelligence agency*". No recommendation from any expert body supports this extension of criminal liability. What this amendment seeks to do is reintroduce de facto a previous deeming element of the current definition of "*security*" at s 121.1 which the INSLM's recommendation requires be repealed. • **Criminal investigations:** The INSLM's recommendation for reforming the criminal investigation limb of the defence by introducing two targeted replacements with a clearer and higher materiality threshold have been ignored. No substantive reasons have been given.
	Penalty should be reduced	ARTK supports the INSLM's recommendation to **reduce penalties**.	AGD considered **no changes** to outsider offences required.	The maximum penalty should be **approximately half** the maximum penalty for a comparable communication by an official (INSLM Rec 12).	Government commits to a penalty of "*approximately half*" of the max penalty for the comparable offence.	ARTK concern addressed in substance: • Penalty has been reduced from 5 to 3 years. The cognate offences at ss122.1 and 122.2 have a penalty of 7 years.

ISSUES		ARTK POSITION (IF ANY)	AGD REVIEW (21 NOVEMBER 2023)	INSLM REVIEW (27 JUNE 2024)	GOVERNMENT RESPONSE TO INSLM REVIEW (27 NOVEMBER 2024)	SECRECY BILL (2026)
	Change fault elements from recklessness to intention in the outsider offence	All harm based elements of this offences **should use as a mental element intention rather than recklessness**. This is because outsiders to government will often appreciate a risk of X occurring (satisfying the recklessness test) but will have no way to confirm one way or the other. For example, rather than the defendant been liable if they are aware of a "*substantial risk*" that information could cause "*serious harm to security*" and proceeding without justification (the recklessness standard), the defendant should only be liable where they believe this circumstance exists or will exist (the intention standard).	AGD considered **no changes** to outsider offences required.	On balance, the **recklessness element should remain**. However there are "*strong arguments*" to use an intention rather than recklessness standard in the outsider offence in s 122.4A . Moving to an intention standard from the current recklessness standard would be recommended if: • The offence continued to use security markings as an element of the offence (which has now been addressed – see Row 11 above); or • The offence of "dealing with" information continued to apply (which has now been addressed – see Row 15 below).	Not dealt with.	ARTK concern not addressed.
	Remove dealing with information as an element of the offence outsider offence	The current two outsider offences in s 122.4A(1) (communicating information) and s 122.4A(2) (dealing with information) duplicate each other. This creates confusion and uncertainty and unfairness as the penalties are different. The overlap occurs because the communication offence incorporates criminal law principles of attempt, which extend that offence to activities taking place before information is communicated. Such activities are separately covered by the "dealing with" offence.	AGD considered no changes to outsider offences required.	The offence for 'dealing with' information by non-officials in s 122.4A(2) should be repealed (INSLM Rec 8).	Agreed.	ARTK concern addressed.
Criminal Code s 122.5(6) — Journalist protection	**The journalist protection should be recast as an exception. An evidentiary onus should not sit on the defendant.**	This protection should be reframed as follows: • **Defence vs Exception**: the journalist protections should be reframed as an exception to the offence, rather than as a defence as currently. This is to signal better that journalism is not, prima facie, a crime and that criminal investigations should not proceed on the assumption that it up to the journalist at the end of the process to prove that the journalist protection applies as a "defence" – rather the existence of the journalist protection must be fully considered at all stages of the investigation to encourage early discontinuances when it becomes obvious the journalist protection is available. • The Law Council has similar concerns. • **Onus of proof**: regardless of whether the protection is framed as an exception or defence, no evidential onus should be placed on the defendant to establish that the protection applies. Placing an evidential onus on the defendant in the context of this legislation is not consistent with established legislative scrutiny principles. It also puts a defacto duty on the journalist to go into evidence, violating their right to silence and jeopardizing their confidential sources.	AGD: • **Defence vs Exception**: Asserts without explanation that "*defence*" terminology for journalist protection is appropriate (AGD [213] – [214]) • **Onus of proof**: AGD appears to concede that scrutiny principles that deal with imposing evidentiary onuses have not been satisfied, and instead asserts that placing an evidential onus on the accused is nonetheless needed because of the open-ended nature of the defence (AGD [210]-[212])	Amendments are potentially warranted: • **Defence vs Exception:** Consideration should be to recasting the current defence as an exception; • **Onus of proof**: INSLM declined to make a recommendation for change based primarily on the international law position concerning evidentiary onuses. The INSLM did not apply relevant legislative scrutiny principles in his analysis. (INSLM Rec 13)	Agrees.	ARTK concern not addressed. ARTK is not aware of the outcome of the "consideration" which the Government committed to give the issue of recasting the journalist defence as an exception.
	The journalist protection should apply to all Commonwealth secrecy offences	The journalist protection in s 122.5(6), as properly reformulated, **should apply to all secrecy offences** across the Commonwealth statute book. It is incongruous to apply the current defence to all offences in Criminal Code Part 5.6 but not to overlapping or lesser offences outside Part 5.6. Public interest journalism cannot efficiently occur in	The appropriateness of a journalist defence should be considered when offences are created – i.e. no review of *existing* offences was required to evaluate whether a journalist protection was required.	Matter out of scope of INSLM review. Recommendations one way or the other could not be expected.	Matter out of scope of INSLM review – so not addressed in Government response.	ARTK concern not addressed. The reasons given for not extending the current journalist defence are incorrect: • The SoC asserts that the offences outside Part 5.6 do not apply to journalists. This is incorrect because of the principles of extended criminal liability in Part 2.3 of the Criminal Code which in many situations will

ISSUES		ARTK POSITION (IF ANY)	AGD REVIEW (21 NOVEMBER 2023)	INSLM REVIEW (27 JUNE 2024)	GOVERNMENT RESPONSE TO INSLM REVIEW (27 NOVEMBER 2024)	SECRECY BILL (2026)
		an environment when any publication remains subject to over 520 retained criminal offences.				apply secrecy offences not specifically covering journalists to journalists. This is why the current offences in Criminal Code s122.1 and s 122.2 – which on their face do not apply to journalists – are all made subject to the current journalist defence. • The SoC also asserts that the information covered by the remaining 520 + offences relates to "*sensitive information*" – this appears to not be the case. But to the extent it is, the more serious offences in Part 5.6 apply to the same kinds of information or to more serious kinds of information, and these Part 5.6 offences are already subject to a journalist defence.
	Extended criminal liability should not apply to secrecy offences	Criminal Code Part 5.6 is divided into two types of offences: offences for commonwealth officers and contractors (ss 122.1, 122.2, 122.4) and outsider offences (s 122.4A)). The outsider offences applicable to journalists and other civil society actors are significantly more narrow. However, if extended liability under Part 2.4 of the Criminal Code were to apply, outsiders could be tried under the insider offences. This defeats the point of having much more targeted offences for insiders.	Not dealt with.	INSLM did not support a change to the ordinary operation of Part 2.4 of the Criminal Code (the accessorial liability provisions).	Not dealt with.	ARTK concern not addressed.
	Wider public interest defence	ARTK does not take a position on this issue.				
Criminal Code s AG Consent – Criminal Code s 123.5	**Correction of existing drafting defects and extension of AG consent requirement across the statute book**	• **Fixing drafting**: the current AG consent requirement applicable to prosecutions under Criminal Code Part 5.6 contains a drafting error that excludes prosecutions brought summarily. • **Extending the requirement**: while the extension of the AG consent requirement to all secrecy offences outside Part 5.6 provides a further, limited protections to journalists, it is not an answer to legitimate journalist concerns that arise from overbroad, indeterminate secrecy laws exceeding 520+ in number. ARTK does however welcome the measure as one limited step in the right direction. • ARTK notes that the requirement for AG consent is already *apparently* provided for by Ministerial direction issued under s 8 of the *Director of Public Prosecutions Act 1983* (Cth). ARTK has not been able to locate a published copy which is concerning from a rule of law perspective.	AGD: • Agrees it is appropriate to retain the requirement for the Attorney General's consent for a journalist to be prosecuted for secrecy offences; and • **Extending the requirement**: notes that the requirement for consent outside the current Part 5.6 offences remain in the form of a ministerial direction, rather than being legislated (AGD [226]).	INSLM: • **Fixing drafting:** recommended amending consent requirement so that it applies regardless of whether the prosecution proceeds by way of committal or summary proceedings (currently, s 123.5 only applies to committal proceedings and does not cover summary prosecutions). • **Extending the requirement**: recommended retaining the requirement for the Attorney-General's consent for prosecution under Part 5.6. (INSLM Rec 14). Note: whether to extend the consent requirement beyond Criminal Code Part 5.6 was largely beyond the INSLM's terms of reference. Recommendations one way or the other could not be expected.	Agreed	ARTK concerns addressed – in so far as this measures provides a further, very limited protections to journalists
Failure to repeal secrecy offences	**Ongoing application of sunsetting version of s 122.4 through savings provisions to 11 confidentiality duties**	There is no acceptable justification given for why 11 existing non-disclosure duties are subject to ongoing criminalisation under a retained version of the previous version of Criminal Code s 122.4. There is no principled basis for extending criminal liability in this way.	Not dealt with.	Not dealt with – beyond scope of INSLM review.	Not dealt with.	Concern not addressed.

ISSUES		ARTK POSITION (IF ANY)	AGD REVIEW (21 NOVEMBER 2023)	INSLM REVIEW (27 JUNE 2024)	GOVERNMENT RESPONSE TO INSLM REVIEW (27 NOVEMBER 2024)	SECRECY BILL (2026)
	Failure to repeal 520 + secrecy offences	ARTK suggests **5 core principles** which should govern whether secrecy provisions are created or otherwise preserved in Australia: 1. All non-disclosure/secrecy offences must protect the paramount importance of the Australian people's right to know about the conduct of its own government. This requires robust journalist protections. 2. Any criminal sanction must require an intention to cause harm to a recognizable public interest. 3. There must be clear, meaningful, and serious harm to a recognisable public interest, and any criminal sanction must be proportional to address that harm. Those recognised public interests have been set out in the earlier ALRC report and the more recent INSLM report. 4. Those offences that remain generally need updating so that they cohere with the Criminal Code and are interoperable with the offences in Part 5.6 and adopt standardised approaches to defences, exceptions, facilitation of proof and mental and physical elements 5. Any offences that remain should not overlap with Part 5.6 offences – there is a compelling interest in ensuring as low a number of offences on the statute book as possible.	Not dealt with, save for generic statements about the need for a harm element to all secrecy offences.	Generally not dealt with directly: • the interaction with the Part 5.6 offences and the broader Commonwealth statute book was generally beyond scope of the INSLM review. Recommendations one way or the other were could not be expected. • INSLM did make recommendations to narrow deemed harm offences in the *Intelligence Services Act 2001*, the *Australian Security Intelligence Organisation Act 1979*, and the *Office of National Intelligence Act 2018* (INSLM Rec 4).	The Government: • did not agree with INSLM's proposed changes to the IS Act, the ASIO Act, and the ONI Act, such that those offences be narrowed as described in INSLM Recommendation 2, stating that "secrecy obligations applying to staff, affiliates and individuals who have entered into contracts, agreements or arrangements with ASIS, ASIO, ASD, AGO, DIO and the ONI should be stricter than secrecy obligations applying to other Commonwealth officers" (Government Response, p 4).	Concern not addressed. Bill appears to repeal only 29 offences.