Australian Government

Independent National Security Legislation Monitor

Secrecy Offences

Review of Part 5.6 of the *Criminal Code Act 1995*

INSLM

Jake Blight

Independent National Security Legislation Monitor (INSLM) Report

Secrecy Offences – Review into Part 5.6 of the *Criminal Code Act 1995*.

978-1-921241-90-1 (Print)

978-1-921241-91-8 (Online)

Copyright

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (www.dpmc.gov.au/government/commonwealth-coat-arms).

Acknowledgement of Country

The Independent National Security Legislation Monitor and the INSLM Office acknowledge the custodians of the lands on which we work and their contribution to our communities. We pay our respect to Elders past and present, and extend this respect to Aboriginal and Torres Strait Islander people across this nation, who hold the memories, traditions, cultures and hopes of Aboriginal and Torres Strait Islander peoples.

Through our reviews and recommendations, the Monitor and INSLM Office seek to ensure Australia's national security and counter terrorism legislation remains proportionate to the threats these laws were designed to address and achieves an appropriate balance between national security and individual rights. As an organisation focused on law and law reform, we acknowledge that Aboriginal and Torres Strait Islander peoples have had a continuing system of law on these lands for tens of thousands of years.

Australian Government
Independent National Security Legislation Monitor

31 May 2024

The Hon Mark Dreyfus KC MP

Attorney-General

Parliament House
CANBERRA ACT 2600

Dear Attorney-General,

Report into Part 5.6 of the *Criminal Code Act 1995*

Pursuant to s 6(1B)(c) of the *Independent National Security Legislation Monitor Act 2010* (Cth) (*INSLM Act*), I have reviewed the operation, effectiveness and implications of Part 5.6 of the *Criminal Code Act 1995* (Cth).

In my view, this report does not contain information of the kind referred to in s 29(3) of the *INSLM Act* and is suitable to be laid before both Houses of Parliament.

Yours sincerely

Jake Blight

Independent National Security Legislation Monitor

In our society, threats to the rule of law are not likely to come from large and violent measures. They are more likely to come from small and sometimes well-intentioned encroachments upon basic principles, sometimes by people who do not understand those principles.

The Honourable Chief Justice (Anthony) Murray Gleeson

Official secrecy has a necessary and proper province in our system of government. A surfeit of secrecy does not.

The Honourable Justice Paul Finn

Table of Contents

Overview and recommendations

There is some information that, in the wrong hands, could genuinely harm Australia's national interests. Secrecy offences that criminalise unauthorised dealing with and communication of this type of information have a role to play in deterrence and punishment. This review considers whether the offences in Part 5.6 of the *Criminal Code* operate in a way that is effective, necessary, proportionate and consistent with Australia's international obligations; and whether the offences contain sufficient safeguards.

There are problems with the current offences, and these need to be addressed. For example, there is significant uncertainty as well as conflict with rule of law principles because of the way a policy framework is used to define key elements of some offences. There are also problems with proportionality in penalising non-officials, particularly in relation to receiving or otherwise dealing with information. The recommendations of this review will ensure that information which is or is likely to be harmful to critical national interests remains protected but in a way that is clearer and more consistent with the rule of law and concepts of necessity and proportionality; and with Australia's international obligations.

This report begins with an overview of the context in which Part 5.6 of the *Criminal Code* operates and key definitions (**Chapter 1**), the current threat environment (**Chapter 2**) and international obligations (**Chapter 3**). **Chapter 4** then considers the main deemed harm offence, finding it uncertain, inconsistent with key rule of law principles and unreasonably broad. **Recommendations 1–5** are made to address these concerns, the most important being the removal of reliance on security classification markings as an element of an offence. Harm-based and related offences for officials are analysed in **Chapters 5–7**. **Recommendations 6, 7, 9** and **10** are directed at improving these, including by clarifying definitions and ensuring a cascading approach to penalties. **Recommendation 11** sets out principles for a replacement general offence for officials. A key recommendation concerning offences for non-officials is removing 'dealing with' offences (**Recommendation 8**) along with refining the circumstances in which a disclosure offence occurs (**Recommendation 12**). While there is some scope to recast the defence for journalists as an exception, it is not recommended that a general public interest test or element be introduced (**Recommendation 13**). Safeguards in both policy and the legislation are discussed in **Chapter 10**, with some enhancements suggested (**Recommendations 14** and **15**).

In conducting this review, I consulted with a range of stakeholders, published a detailed Issues Paper, held individual and roundtable meetings, received 22 written submissions, held 2 days of public hearings, received 4 supplementary submissions and responses to questions on notice from 6 agencies. I was greatly assisted by considered submissions from non-government organisations, government agencies and academics as well as by counsel and INSLM staff. I thank all of those who have been involved in the review.

Deemed harm offences for Commonwealth officials

Deemed harm offences do not require proof of any actual harm or risk of harm. They should only be used for information that is always, or almost always, going to be harmful to a critical national interest if disclosed. The current deemed harm offence in s 122.1 of the *Criminal Code* applies to three broad categories of information: any information that has been classified as secret or top secret; any information obtained or made by or for one of Australia's 6 main intelligence agencies or any foreign intelligence agency in connection with its functions; and any information about the operations, capabilities or technologies of, or methods or sources used by, any domestic or foreign law enforcement agency.

Security classified information

Relying on classification markings to guide how officials use, store and disseminate information is a longstanding and reasonable policy. However, seeking to incorporate a policy directly into the criminal law raises many legal issues.

Information is 'security classified' if it has a security classification applied 'in accordance with' a policy framework. There is real uncertainty about when a classification is applied 'in accordance with' the policy framework. Not all information marked 'secret' or 'top secret' will meet the legal test. It is likely that evidence will need to be led in a prosecution to establish that disclosure of the information would be expected to cause serious or grave damage to specified interests. The current policy framework lacks the precision expected for criminal law and parts appear inconsistent with the requirements in the *Criminal Code*. Training, record-keeping and review procedures are inadequate when it comes to making decisions that have such significant criminal law implications. These things may not be necessary for a policy that has only administrative consequences, but should be in place for decision-making that has such serious criminal law consequences.

Even if more certainty could be injected into classification decision making there are fundamental rule of law issues with having, as a core element of an offence, decisions made under a policy framework. This is because the executive can change policies at any time. It is also problematic that parts of the relevant policy framework are not publicly available. Furthermore, reliance on a policy document to frame a criminal offence may not be compliant with Australia's international obligation that limits to the freedom of expression can only be imposed *by law*.

RECOMMENDATION 1: The offences in Part 5.6 should not rely on information being classified under a policy framework as an element of the offence.

Removing classification markings as a physical element of the offences does not mean that they have no role to play whatsoever. A classification marking combined with evidence of an official's training and experience in what those markings indicate, would go a long way towards establishing, as matter of fact, the required fault element of recklessness.

Information about intelligence agencies

Disclosure of information about the core intelligence operations, capabilities, technologies, methods and sources of Australia's 6 main intelligence agencies will almost always be harmful to the national interest. But it does not follow that *all* information to do with those agencies will always be harmful. This is particularly so for agencies whose functions have expanded beyond traditional intelligence functions and now include assisting other bodies – such as the Department of Home Affairs – with their functions; undertaking broad cybersecurity functions; or some commercial mapping. The same is true for routine administrative and corporate information. Disclosure of information about non-intelligence functions and administrative activities *can* result in harm in *some* circumstances but not with the degree of certainty that justifies a deemed harm offence. Where disclosures about these other activities cause harm or are likely to cause harm to security, defence or international relations, they will be covered by the harm-based offence in s 122.2 (**Recommendation 6**).

RECOMMENDATION 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.

For ASIS, ASD, AGO and DIO, 'intelligence information' should be defined by reference to the existing definition of 'intelligence information' in the *Intelligence Services Act*. For ASIO, it should cover information obtained for the purpose of security (as defined in the *ASIO Act*), as well as ASIO's foreign intelligence function in s 17(1)(e) of that Act. For ONI, the definition of 'intelligence information' should be linked to ONI's statutory intelligence functions in s 7(1)(c)(d)(e) and (g) of the *ONI Act*. The inclusion of DIO in this offence is contingent on **Recommendation 5**.

Law enforcement – electronic surveillance capabilities

Any intentional or reckless interference with the integrity of the criminal justice system or disclosures that would undermine law enforcement capabilities are serious and deserve some type of sanction. However, it does not follow that it is necessary and proportionate for *all* information relating to the operations, capabilities, technologies, methods or sources of *any* agency with a role in enforcing the criminal law to be covered by a broad 7–10-year deemed harm offence. This covers many agencies and a very large amount of information, not all of which is particularly sensitive.

This review recommends a cascading approach. The serious deemed harm offence in s 122.1 should apply to the technologies, capabilities and methods that support the extraordinary electronic surveillance powers that parliament has granted to a small number of agencies to combat serious crimes. These surveillance capabilities include remote computer access, telecommunications interception, network access and account takeover warrants. The

specialised capabilities needed to use these powers require significant investment. They would take a long time to replace if compromised, and their loss would seriously undermine the ability to combat serious and organised crime. Other types of interference with the criminal justice system are dealt with in **Recommendations 6** and **11**.

RECOMMENDATION 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.

Overlapping offences for intelligence agency information

There is almost complete overlap between agency-specific secrecy offences for ASIS, ASD, AGO, DIO, ONI and ASIO and the general offence in s 122.1. Those agency-specific offences presently apply to *any* information made by or for the agency in connection with its functions. For the same reasons discussed in relation to **Recommendation 2**, this is excessively broad and these offences should be narrowed in the way proposed by **Recommendation 2**.

There is a good argument for repealing the agency-specific secrecy offences and instead relying on the *Criminal Code*. This would be consistent with the goal of reducing the overall number of secrecy offences. Some care in drafting would be required to ensure that all individuals presently covered by the offences (such as ASIS agents) would continue to be covered by the new offence and that new defences were not added without consideration of whether they were appropriate. The penalties are already similar.

Most of the intelligence agencies oppose moving their general secrecy offences into the *Criminal Code*, primarily because they consider additional defences should not be available. For example, Part 5.6 of the *Criminal Code* includes defences for lawyers who provide legal advice on offences against that Part and in relation to information that has been previously published. It may complicate the drafting in the *Criminal Code* for some defences not to be available to people who would otherwise fall into the definition of 'Commonwealth official' or persons otherwise performing work for the Commonwealth.

There are some very specific matters that apply to ASIS and ASIO that should be retained as specific offences in their own Acts. In particular, ASIS and ASIO staff and agents undertake covert intelligence collection activities that put them in positions of particular risk if their identities are disclosed.

ASIO's new function of assessing and granting the highest level of security vetting clearances also presents a particular risk. This information should be covered in the *ASIO Act* for ASIO staff and affiliates. For other Commonwealth officials, disclosure of vetting information should be covered by the harm-based offences in ss 122.2 and 122.4.

RECOMMENDATION 4: If separate general 'deemed harm' offences are to be retained in the *Intelligence Services Act 2001*, the *Australian Security Intelligence Organisation Act 1979* and the *Office of National Intelligence Act 2018*, 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.**
- **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 under Part IVA of that Act.**

Defence Intelligence Organisation needs statutory functions

Currently the *Criminal Code* and the *IS Act* both describe serious criminal offences by reference to DIO's functions. Those functions are not set in legislation; they are set by a policy document, generated by the Department of Defence, that can be changed at any time. It is not appropriate for the scope of a serious criminal offence to be changeable in this way.

Setting out the functions of DIO in legislation or a disallowable legislative instrument would also provide for parliamentary oversight and clarity in the operation of the exceptions for DIO in the *FOI Act*, *Privacy Act* and the way DIO information is dealt with in the *PID Act*.

RECOMMENDATION 5: The functions of the Defence Intelligence Organisation should be set out in legislation or in a disallowable legislative instrument.

If this recommendation is not accepted, I recommend that the *IS Act* be amended to repeal the secrecy offences for DIO and that s 122.1 of the *Criminal Code* not refer to DIO, as both offences are dependent on the scope of DIO's functions. The disclosure of DIO information which is likely to harm security, defence or international relations would continue to be covered by the offence in s 122.2.

Harm-based offence for Commonwealth officials

The offence in s 122.2 is a 7-year (or 10-year in aggravating circumstances) harm-based offence. It applies when an official is reckless as to whether their conduct will cause harm, or is likely to cause harm, in a range of circumstances. The offence should be retained but requires increased clarity as to what is meant by 'security', 'defence' and 'international relations'. There should be a cascading approach to law enforcement capabilities.

'Security' should be defined in accordance with the definition in the *ASIO Act*. 'Defence' should be defined in a way that incorporates functions directly connected to the defence of

Australia, such as those described in recommendation 2.3 of the October 2023 INSLM NSI Act Report. 'International relations' should cover diplomatic and military relations with foreign governments and international organisations, including bilateral and multilateral law enforcement and intelligence cooperation arrangements.

The offence in s 122.2 should penalise disclosures that could compromise the utility of powers exercised under warrants and authorisations granted to support the investigation of crime by any agency. This includes capabilities connected to statutory powers to access information or to search people, places or things – for example, sensitive forensic capabilities used to extract information from items seized under a search warrant. Other types of interference with the criminal justice system are dealt with in **Recommendations 3** and **11**.

RECOMMENDATION 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.**

'Dealing with' offences

The 'dealing with' offences penalise conduct even when a person does not intend to disclose information. The definition of 'deal' is long and contains overlapping categories. A person deals with information if they receive or obtain it; collect it; possess it; make a record of it; copy it; alter it; conceal it; communicate it; publish it; or make it available.

For the officials that the Commonwealth trusts to access the type of information covered by the revised ss 122.1 or 122.2, a 'dealing with' offence can be justified in most circumstances. With the exception of removing the initial receipt of information, this recommendation is intended to refine the definition and remove overlap, not to substantially alter the existing offence for officials.

RECOMMENDATION 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.

Non-officials are in a different position from officials when it comes to assessing when criminal sanctions are justified. Non-officials do not have the same duty to protect Commonwealth information that officials do.

A non-official who attempts a disclosure or commits other ancillary offences (such as inciting an official to make an unlawful disclosure) is already subject to other criminal offences. If they act on behalf of a foreign principal or for espionage, a range of criminal offences apply. Depending on the specific facts, it is possible that possession of stolen property offences may also apply.

Considering the position of non-officials compared to officials and the range of other existing offences, it is not proportionate to apply 'dealing with' offences to non-officials. Disclosure offences should continue to apply as per **Recommendation 12**.

RECOMMENDATION 8: The offence for 'dealing with' information by non-officials in s 122.4A(2) should be repealed.

Proper place of custody

There are offences that were intended to apply to officials who remove information from a 'proper place of custody'. These offences are not operational because, in the almost 6 years since they were enacted, regulations to define 'proper place of custody' have never been made. The offences are not necessary and should be repealed.

RECOMMENDATION 9: The 'proper place of custody' offences in ss 122.1(3) and 122.2(3) should be repealed.

Aggravating offences

Currently there are 4 circumstances in which an offence by an official under ss 122.1 or 122.2 becomes an aggravated offence. Most should be repealed, as they are uncertain or arbitrary or are part of the aggravating circumstances already considered as part of sentencing, including those associated with dishonesty, gravity and scale.

There are 2 circumstances where a penalty beyond the maximum of 7 years (for communicating) or 3 years (for dealing) is justified. The first is where an official holds the highest level of security clearance. Those with the highest level of clearance have qualitatively and quantitively different access to sensitive information than those with lower clearances or no clearance. There is also a particular harm to the Commonwealth and its relationship with foreign partners if there is a breach of trust by those granted the very highest level of security clearance. A higher maximum penalty can also be justified where a person acts with an *intention* or *knowledge* that their conduct will or is likely to cause harm.

RECOMMENDATION 10: 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 where the person intended or knew their conduct would or was likely to cause a type of harm covered by the underlying offence.

General offence for Commonwealth officials

The general offence for officials in s 122.4 is due to sunset in December 2024. The Attorney-General's Department has recommended it be replaced by a new general offence. Policy and drafting work is ongoing. This recommendation can provide only in-principle guidance.

RECOMMENDATION 11: Any general offence to replace s 122.4 should be consistent with the following principles:

- **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.**
- **The offence should be harm-based and relate to essential public interests. However, if 'deemed harm' offences are to be incorporated, they should be limited to a very narrow category of information where significant harm to an essential public interest is always, or almost always, going to be the result.**
- **The offence should cover only disclosures that cannot be adequately dealt with by existing remedies including contractual and administrative remedies.**
- **Broad and uncertain language such as 'functioning of government' should be avoided.**
- **The offence should apply to current and former Commonwealth officials and others who perform work for a Commonwealth entity in relation to information acquired in the course of their duties. However, if the scope of the offence is to be broadened it should still be closely linked to some kind of contract, agreement or arrangement with the Commonwealth.**
- **The penalty for reckless conduct should be no more than 2 years imprisonment.**

If a primary justification for the new general offence is to replace specific existing offences then the offences to be repealed should be included in the legislative proposal in order to allow parliament to properly assess the necessity and proportionality of the new offence.

Offence for non-officials

The offence in s 122.4A applies to non-officials, including journalists. For the reasons applicable to **Recommendation 1**, using 'classified information' as an element of the offence creates significant uncertainty and real concerns with the rule of law. These are even more profound for non-officials. The remaining categories in the existing offence require revisions to bring them into line with other recommendations in this report and to ensure that the threshold for liability for non-officials is higher than for officials.

RECOMMENDATION 12: The offence in s 122.4A for communications by non-officials should be modified so that:

- **classification markings do not form an element of the offence**
- **the current requirement that actual harm be established should be maintained and the offence apply to:**
  - **causing serious damage to the security or defence of Australia, with those terms defined as per Recommendation 6**
  - **seriously undermining the utility of the technologies, capabilities and methods used to exercise special statutory powers (per Recommendations 3 and 4)**
  - **seriously impeding the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth**
  - **prejudicing the health or safety of the Australian public or a section of the Australian public.**
- **the maximum penalty should be approximately half the maximum penalty for a comparable communication by an official.**

Action should be taken to ensure that ABC and SBS staff and contractors are not inadvertently covered by the offences for officials as persons 'otherwise engaged to perform work for a Commonwealth entity'.

Journalism and public interest defences

Several non-government organisations made strong arguments as to why a public interest test should be added as an *element* of secrecy offences and/or that a general public interest *defence* should be added. There is merit in these arguments. However, it would be complex and uncertain in practice. There are likely to be many competing public interests at play, some of which may shift over time. A general public interest element or defence for officials

would also undermine the parliamentary intention that there be specific statutory mechanisms for providing immunity to those who bring forward wrongdoing.

Concerns about 'dealing with' information by journalists, lawyers and civil society groups will be dealt with by **Recommendation 8**. However, if that recommendation is not accepted, additional changes to some defences will be needed.

The current defence for disclosures in the course of reporting news and current affairs should be retained. For a journalist to invoke the defence, they must adduce or point to evidence that, taken at its most favourable, suggests a reasonable possibility that they 'reasonably believed that engaging in the conduct was in the public interest'. This is known as an 'evidential burden' and is not a high bar. Once it is discharged, the prosecution must prove beyond reasonable doubt that each element of the defence does not exist. In the full context of how criminal trials operate in Australia, this approach remains reasonable.

Nevertheless, there may be value in reframing the current 'journalist defence' as an exception rather than as a defence. Although the value would primarily be symbolic, it may make clearer that a reasonable belief that conduct is in the public interest is something that can be relied on by a journalist to avoid a conviction.

RECOMMENDATION 13: A new general public interest defence or element should not be added in Part 5.6. However, consideration could be given to recasting the current defence for journalists as an exception rather than a defence.

Role of the Attorney-General

The Attorney-General's consent should be required for all prosecutions under Part 5.6. The consent requirement may not currently apply to a prosecution that proceeds summarily because consent is triggered by 'commitment' which occurs only for trial by indictment.

Before any prosecution based on information being 'security classified' the Attorney-General must certify that it was appropriate that the information had a security classification. If **Recommendation 1** is accepted and security classification is no longer an element of any offence then this requirement will fall away; otherwise, it should be retained.

RECOMMENDATION 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.

Prosecution Policy of the Commonwealth

The Prosecution Policy of the Commonwealth contains a non-exhaustive list of factors that the Commonwealth Director of Public Prosecutions (CDPP) is to take into account when considering the public interest in a prosecution. Prosecutions for secrecy offences can require consideration of the role of a free press including in exposing corruption or other wrongdoing by government officials. While the CDPP can already take this into account under the general concept of public interest, there is merit in explicitly including it in the list of public interest factors to be considered.

RECOMMENDATION 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.

Chapter 1: Scope and context for this review

1.1 This is a report of an independent review of the secrecy offences in Part 5.6 of the *Criminal Code Act 1995* (Cth) (*Criminal Code*). The review was conducted between December 2023 and May 2024 under the *Independent National Security Legislation Monitor Act 2010* (Cth) (*INSLM Act*). Part 5.6 of the *Criminal Code* as in force at the time; together relevant with definitions from that Act and other Acts, is in **Annex A**.

1.2 This chapter begins by briefly describing the role of the Independent National Security Legislation Monitor (INSLM) and the things that an INSLM review is required to consider. The chapter then notes the growth in the number of secrecy offence provisions and the history of reviews of these types of offences (also see **Annex B**). Some statistical information is provided about secrecy offence reports to the Australian Federal Police (AFP) and referrals to the Commonwealth Director of Public Prosecutions (CDPP). Information is also provided about the use of administrative sanctions within National Intelligence Community (NIC) agencies. At the end of the chapter there is a discussion about who is a 'Commonwealth officer or a person otherwise engaged to perform work for a Commonwealth entity' – a category of people central to most of the offences in Part 5.6.

The role and functions of the INSLM

1.3 The Independent National Security Legislation Monitor (the Monitor) is a statutory office holder who independently reviews Australia's national security and counterterrorism laws and can make recommendations for law reform.

1.4 The Monitor can initiate certain reviews of their own motion or have a matter referred by the Prime Minister, the Attorney-General or the Parliamentary Joint Committee on Intelligence and Security (PJCIS). The *INSLM Act* also requires the Monitor to undertake certain reviews.[1]

1.5 INSLM reviews consider the operation, effectiveness and implications of the relevant law and whether it contains appropriate protections for individual rights, remains necessary and proportionate and is consistent with Australia's international obligations.[2]

1.6 The Monitor has powers to access any material they consider relevant, including classified information, and can determine their own review process. The process of this review is described in **Annex C**.

---

1 *Independent National Security Legislation Monitor Act 2010* (Cth) ss 6–7A ('*INSLM Act*').
2 *INSLM Act* (n 1) ss 6(1), 8.

Timing and scope of this review

1.7 The *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth) (*EFI Act*) and the *Foreign Influence Transparency Scheme Act 2018* (Cth) were introduced concurrently to address the increasing threat of espionage and foreign interference.[3] One goal of the legislative package was to criminalise the unauthorised disclosure of information. The new laws also included provisions requiring those holding foreign interests and engaging in the Australian political landscape to register those interests.[4] There were also new offences to 'criminalise covert, deceptive and threatening actions by persons acting on behalf of, or in collaboration with, a foreign principal aiming to influence Australia's political processes or prejudice our national security'.[5]

1.8 The *EFI Act* amended the *INSLM Act* to require the Monitor to review the following elements of Chapter 5 of the *Criminal Code* that were added or amended by the *EFI Act*:

- sabotage (Division 82)
- espionage and related offences (including foreign interference offences) (Part 5.2)
- secrecy of information (Part 5.6).

1.9 The *INSLM Act* requires these reviews to start as soon as practicable after the third anniversary of the *EFI Act* receiving Royal Assent.[6]

1.10 I commenced as the fifth Monitor on 26 November 2023 and promptly began scoping the reviews required by the *INSLM Act*. I decided to begin with reviewing the secrecy offences in Part 5.6, partly because at that time the first trial for a foreign interference offence under Part 5.2 was in progress – I considered it prudent to await the outcome of that case and any appeal before commencing a review of how the foreign interference and closely related espionage and sabotage laws are operating.[7] The other reason I prioritised reviewing the

---

3 Commonwealth, *Parliamentary Debates*, House of Representatives, 7 December 2017, 13147–13148 (Malcolm Turnbull, Prime Minister).

4 Commonwealth, *Parliamentary Debates*, House of Representatives, 7 December 2017, 13147 (Malcolm Turnbull, Prime Minister). The Foreign Influence Transparency Scheme was recently reviewed by the Parliamentary Joint Committee on Intelligence and Security (PJCIS), which recommended significant changes: see PJCIS, Parliament of Australia, *Review of the Foreign Influence Transparency Scheme Act 2018* (Report, March 2024).

5 Commonwealth, *Parliamentary Debates*, House of Representatives, 7 December 2017, 13147 (Malcolm Turnbull, Prime Minister).

6 *INSLM Act* (n 1) s 6(1B). The *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth) ('*EFI Act*') received Royal Assent on 29 June 2018.

7 That matter subsequently resulted in a conviction and the appeal period has now passed: see *CDPP v Duong* [2024] VCC 182. A second person has been charged with reckless foreign interference and has

secrecy offences is that the general secrecy offence contained in s 122.4 of Part 5.6 is due to sunset on 29 December 2024. An Issues Paper for this INSLM review was published on 19 January 2024.

1.11 On 21 March 2024, in its *Advisory Report on the National Security Legislation Amendment (Comprehensive Review and Other Measures No. 3) Bill 2023*, the PJCIS recommended that the Australian Government consider aligning the Bill's proposed amendments to secrecy offences contained in the *Intelligence Services Act 2001* (Cth) (*IS Act*) and the *Australian Security Intelligence Organisation Act 1979* (Cth) (*ASIO Act*) with the relevant recommendations of this review, pending the timing of completion of this review and passage of that legislation.[8] The Bill passed both houses and received Royal Assent in May 2024, just prior to the finalisation of this report.

1.12 In accordance with ss 6 and 8 of the *INSLM Act*, the review of Part 5.6 must consider:

- the operation, effectiveness and implications of the law
- whether the law contains appropriate safeguards for protecting the rights of individuals
- if the law remains proportionate to any threat of terrorism or threat to national security, or both
- whether the law remains necessary
- Australia's obligations under international agreements, including:
  - human rights obligations
  - counterterrorism obligations
  - international security obligations
- arrangements agreed from time to time between the Commonwealth, the States and the Territories to ensure a national approach to countering terrorism.[9]

1.13 This report records the result of my analysis of each of these issues as well as key points from the submissions, discussions and public hearings that informed that analysis. A summary of the main findings and the recommendations is contained in the Overview and Recommendations section. **Chapters 1–3** contain important background information and **Chapters 4–9** analyse each of the key provisions largely in the order in which they appear in the *Criminal Code*. In considering the way that the law is operating, I have taken into account

indicated an intention to plead not guilty. I am monitoring that case and will take it into account when I commence the review of Division 82 and Part 5.2.

8 PJCIS, Parliament of Australia, *Advisory Report on the National Security Legislation Amendment (Comprehensive Review and Other Measures No. 3) Bill 2023* (Report, March 2024) (*'PJCIS NSLAB3 Report*').

9 *INSLM Act* (n 1) ss 6(1), 8.

key policies that provide some practical safeguards, as well as safeguards in the law itself (**Chapter 10**).

1.14 The *Public Interest Disclosure Act 2013* (*PID Act*) and protections for whistleblowers are closely related to secrecy offences. A well-functioning whistleblower scheme that is easy to navigate and provides appropriate protections for those who wish to identify wrongdoing is an essential part of the overall proportionality of secrecy offences, including those in Part 5.6 of the *Criminal Code*. The *PID Act* is not within the scope of this INSLM review; however, the Attorney-General's Department (AGD) is currently considering further reforms to the *PID Act* and advised me:

> The Australian Government is committed to strengthening the public sector whistleblowing framework, to ensure effective and accessible protections for whistleblowers. The first stage of reforms commenced on 1 July 2023, alongside the commencement of the National Anti-Corruption Commission. Following a consultation process conducted in late 2023, the Government is considering options for further reforms to ensure Australia's public sector whistleblowing framework is accessible and fit for purpose, and appropriate protections are in place for whistleblowers.[10]

I look forward to the outcomes of that important review.

Previous reviews of secrecy offences

1.15 This review builds on several independent, parliamentary and government reviews that have considered Commonwealth secrecy provisions over the past 30 years. Many of the conclusions that those previous reviews reached are just as relevant today as when they were completed. In addition, many previous review recommendations were highlighted in the submissions I received during this review and have influenced my consideration of Part 5.6 of the *Criminal Code*. The key conclusions from these historical reviews, as relevant to this review, are summarised in **Annex B**.

1.16 It is also important to acknowledge that the threat environment, particularly the threat of foreign interference and espionage, has evolved significantly since earlier reviews. According to the Director-General of Security in 2024, more Australians are being targeted for espionage and foreign interference than ever before (see **Chapter 2**).[11]

1.17 The functions of Australia's intelligence agencies have also grown. Since the Australian Law Reform Commission (ALRC) completed its seminal report, *Secrecy Laws and Open*

10 Email from Attorney-General's Department (AGD) to INSLM, 17 April 2014.

11 Mike Burgess, 'Director-General's Annual Threat Assessment 2024' (Speech, Australian Security Intelligence Organisation, 28 February 2024).

Government in Australia (ALRC 2009 Secrecy Laws Report), and even since the introduction of Part 5.6 of the *Criminal Code* in 2018, there has been significant expansion in the functions and size of our main intelligence agencies.[12] This means that, even where previous reviews suggested that offences specific to intelligence agency functions may be appropriate, it is necessary to reconsider these views in light of the expanded functions.

Principles from Attorney-General's Department Review of Secrecy Provisions

1.18 Following a 2023 review by AGD, the government recently endorsed 12 principles to be used in framing secrecy offences and to guide work to reduce the number of such offences:[13]

- 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: contain an express harm element; cover a narrowly defined category of information and the harm to an essential public interest is implicit; or 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.

---

12 See, for example, new or expanded functions in: *Intelligence Services Act 2001* (Cth) ss 6(1)(ba), 6B(1)(ea)-(g), (3), (4), 7(1)(ca), (2), 13A, 13B ('*IS Act*') and the addition of assisting the Department of Home Affairs with its functions as an Australian Signals Directorate (ASD) function by *Intelligence Services Act Regulations 2021* (Cth). See also the expansion of Office of National Intelligence (ONI) functions in relation to enterprise management by the *Office of National Intelligence Act 2018* (Cth) (*'ONI Act*').

13 AGD, *Review of Secrecy Provisions* (Final Report, 21 November 2023) 8 [18] ('*AGD Review of Secrecy Provisions*'). See also Attorney-General (Cth), 'Reforms to Commonwealth Secrecy Offences' (Media Release, 21 November 2023).

- 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*.
- 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.

1.19 These are sound principles and I have considered them in making my recommendations. I have been particularly conscious of Principle 4: that offences should be harm-based except in the narrowest of categories where harm is implicit (see **Chapters 4**, **7** and **8**). That the conduct being regulated should be clear (Principle 8) is an essential element of the rule of law and has also been referred to numerous times in this report (see in particular **Chapters 4–8**). Principles 6, 7 and 11 are particularly relevant to offences and defences that apply to non-officials (see **Chapters 8** and **9**).

Growth in the number of secrecy offences

1.20 Secrecy offences have a long history in Australian law. One of the first laws passed by the Australian Parliament in 1901 included secrecy obligations for officials and offences directed at keeping everything passing through the post or over the new telegraph lines private.[14] The *Crimes Act 1914* (Cth) (*Crimes Act*) contained 2 general secrecy offences.[15] From the 1940s onwards, there was an expansion of Commonwealth regulation, including into the areas of taxation, health, education, welfare, research and trade. These laws often contained specific secrecy offences.[16] In 2018 the *EFI Act* introduced Part 5.6 into the *Criminal Code* and replaced the 1914 secrecy offences, which had remained largely unchanged until that time.[17] At the time of the ALRC 2009 Secrecy Laws Report, there were 506 secrecy provisions. By the

14 *Post and Telegraph Act 1901* (Cth) ss 9, 49, 115–116, 127, sch 2 as enacted.

15 *Crimes Act 1914* (Cth) ss 70, 79 ('*Crimes Act*').

16 John McGinness, 'Secrecy Provisions in Commonwealth Legislation' (1990) 9(1) *Federal Law Review* 49; Justice Susan Kenny, 'Secrecy Provisions: Policy and Practice' (Speech, National Information Law Conference, 24 March 2011) 4; Maureen Henninger, 'Reforms to Counter a Culture of Secrecy: Open Government in Australia' (2018) 35(3) *Government Information Quarterly* 398.

17 In 1960 amendments were made to extend the operation of the s 70 offence in the *Crimes Act* (n 15) so that it also covered former Commonwealth officers.

end of 2023, there were around 875 Commonwealth secrecy offences and non-disclosure obligations.[18]

1.21 These include a large number of secrecy offences that are specific to the NIC. The *ASIO Act* contains specific offences that apply to Australian Security Intelligence Organisation (ASIO) staff and others who have a contract, agreement or arrangement with ASIO. These offences prohibit all unauthorised communication, dealing with or recording of any ASIO information.[19] The *IS Act* contains similar offences for the Australian Secret Intelligence Service (ASIS), Australian Signals Directorate, Australian Geospatial-Intelligence Organisation and the Defence Intelligence Organisation; and the *Office of National Intelligence Act 2018* (*ONI Act)* largely mirrors these for the Office of National Intelligence (ONI).[20] It is also an offence for any person to publish the identity of a current or former ASIO employee or affiliate or identify an ASIS staff member or agent.[21] There are offences specific to the AFP, the Australian Criminal Intelligence Commission and the information dealt with by the Australian Transaction Reports and Analysis Centre, as well as parts of the Department of Home Affairs.[22] The *Surveillance Devices Act 2004* (Cth) and the *Telecommunications (Interception and Access) Act 1979* (Cth) both contain multiple secrecy offences.[23] Then there is the *Defence Act 1903* (Cth), the *Crimes Act*, other parts of the *Criminal Code* and the *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth).[24]

1.22 When it comes to national security-related matters, there are broad exceptions from the laws that ordinarily allow people access to government information, including the *Administrative Decisions (Judicial Review) Act 1977* (Cth), the *Freedom of Information Act 1982* (Cth), the *Archives Act 1983* (Cth) and the *Privacy Act 1988* (Cth). The *PID Act* scheme provides very

---

18 *AGD Review of Secrecy Provisions* (n 13) 4 [3].

19 *Australian Intelligence Security Intelligence Organisation Act 1979* (Cth) ss 18–18B ('*ASIO Act*').

20 *IS Act* (n 12) s 39–40M; *ONI Act* (n 12) ss 42–44.

21 *ASIO Act* (n 19) ss 92-92A; *IS Act* (n 12) s 41.

22 *Australian Federal Police Act 1979* (Cth) ss 40ZA, 60A; *Australian Crime Commission Act 2002* (Cth) ss 21C(1), (3), (5), 25A(14), 29B(1), (3), 51, 59AB(7)–(8); *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) ss 121(1), (5), (6), 123(1)–(2), (5C), (7AA), (7AC), (7B), (8A), 126(1), (4), 128–129, 207, 35H(1), 35J, 35K(1), 50A(1). There are a range of potentially relevant offences, including *Australian Border Force Act 2015* (Cth) s 42; *Migration Act 1958* (Cth) ss 33(7), 46A(5), 46B(5), 72(5), 91F(4), 91L(4), 195A(7).

23 *Surveillance Devices Act 2004* (Cth) ss 45(1), (2), 45B (1), (2); *Telecommunication (Interception and Access) Act 1979* (Cth) ss 63(1), (2), 181A(1), (2), (4), (5), 181B(1), (2), (4), (5), 133, 182, 182A(1), (2), sch 1 s 152.

24 *Defence Act 1903* (Cth) ss 73A(1), (2), 90, 110XD(2); *Crimes Act* (n 15) ss 3ZQJ, 3ZQT, 3ZZHA, 3ZZVH, 15HK, 15JQ, 15JR(1), 15LC, 15MS, 23XG, 23XH, 23YO; *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth) pt 5.

limited disclosure options for 'intelligence information' – a term given an extraordinarily broad meaning in the *PID Act*.[25]

1.23 Some secrecy in the area of national security, defence, international relations and law enforcement is not without purpose. During the Royal Commission on Australia's Security and Intelligence Agencies, conducted in the 1980s, Justice Hope found that 'the disclosure of secrets … can result in just as much damage to the national interest as can result from espionage or sabotage'.[26] That remains true today. But it is also true that an excess of secrecy can undermine accountability and public trust in government. Both of these threats are discussed in **Chapter 2**.

Investigations and prosecutions

1.24 Despite the large number of secrecy offences, few have been used in prosecutions. According to AGD, in the almost 40 years between 1985 and late 2023, there have been prosecutions in relation to 18 secrecy offence provisions under 11 laws. Primarily, those related to taxation, social security and law enforcement legislation.[27]

1.25 At the time I commenced this review there were 2 high-profile prosecutions on foot: David McBride, who was charged and pled guilty to two counts of unlawful communication under the *Defence Act 1903* (Cth) and one count of theft under the *Criminal Code* (he was sentenced in May 2024);[28] and Richard Boyle, charged with offences under the *Taxation Administration Act 1953* (Cth) and *Listening and Surveillance Devices Act 1972* (SA) (still ongoing at the conclusion of this review).[29] Both matters predate the introduction of Part 5.6 of the *Criminal Code*.

25 *Public Interest Disclosure Act 2013* (Cth) s 41.

26 *Royal Commission on Australia's Security and Intelligence Agencies*: *Report on the Australian Security Intelligence Organization* (Report, December 1984) [9.26].

27 *AGD Review of Secrecy Provisions* (n 13) 11 [25]. See for example, *Grant v Headland* (1977) 17 ACTR 29; *Sherlock v Jacobsen* (1983) 13 ATR 935; *Commonwealth v John Fairfax & Sons Ltd* (1987) 147 CLR 39; *Johnston v Director of Public Prosecutions* (1989) 90 ACTR 7; *R v Crowley* (District Court (WA), Voil DCJ, 17 March 1997, unrep); *R v Kelly* [2006] VSCA 221; *R v Kessing* (District Court (NSW), Bennet DCJ, 22 June 2007, unrep); *R v Goreng-Goreng* [2008] ACTSC 74; *R v Petroulias* [2008] NSWSC 626; *Seivers v The Queen* [2010] ACTCA 9; *R v Scerba* (No 2) [2015] ACTSC 359.

28 *R v McBride (No 4)* [2024] ACTSC 147.

29 See *Boyle v Commonwealth Director of Public Prosecutions* [2023] SADC 27.

1.26 To date, there have been no prosecutions under Part 5.6 since it commenced operation in December 2018.[30]

1.27 According to the recent AGD *Review of Secrecy Provisions*, there has been a 'downwards trend' in referrals of potential breaches of secrecy provisions to CDPP.[31]

1.28 Between 1 January 2019 and 22 February 2024, AFP received 42 external reports for 'information secrecy' or 'unauthorised disclosure' matters under Commonwealth laws; 32 of these matters have been finalised and 10 remain active.[32] Not all of these reports relate to *Criminal Code* offences. In the same period CDPP has received 7 referrals under Part 5.6 of the *Criminal Code*.[33] As at 1 March 2024, CDPP was assessing one brief of evidence for an offence under Part 5.6 of the *Criminal Code*.[34] AFP and CDPP policies which are relevant to assessing investigative priorities and when a prosecution should be initiated are discussed in **Chapter 10**. The fact that only a small percentage of initial reports to AFP ultimately become a brief of evidence for prosecution is not surprising and is true of all crime types, not only secrecy offences.

The use of administrative sanctions in NIC agencies

1.29 Criminal sanctions are not the only response to potential breaches of secrecy obligations by Commonwealth officials and contractors. There are administrative sanctions that can be applied. These range from a warning through to disciplinary processes, security clearance revocations and loss of employment or contract termination. In the context of this review it was not possible, or necessary, to seek to undertake comprehensive research on the interaction between administrative and criminal sanctions in the Commonwealth public sector.

1.30 Instead, evidence was sought from the 10 agencies that make up the NIC about how, in practice, administrative and criminal sanctions operate together in their agency. Each agency was asked to provide statistics on how many and what sort of secrecy-related matters have been investigated internally in the 5 years since the *EFI Act* commenced; how many of those (if any) have been reported to AFP; whether those reports (if any) are likely to proceed to

30 Commonwealth Director of Public Prosecutions (CDPP), *Submission 20*, 1. There was one case where a witness claimed the privilege against self-incrimination with reference to s 122.4: see *Roberts-Smith v Fairfax Media Publications Pty Ltd (No 28)* [2022] FCA 115.

31 *AGD Review of Secrecy Provisions* (n 13) 11 [25].

32 Australian Federal Police (AFP), *Submission 18*, 5. Note that not all of these matters relate to Part 5.6 of the *Criminal Code Act 1995* (Cth) ('*Criminal Code*'). See also Ms Krissy Barrett, Acting Deputy Commissioner, AFP, *Public hearing transcript,* 25 March 2024, 90.

33 A referral includes requests for the CDPP to provide pre-brief advice or for the CDPP to assess a brief of evidence in accordance with the Prosecution Policy of the Commonwealth (see Chapter 10). A referral does not mean that a prosecution will necessarily commence.

34 CDPP, *Submission 20*, 2.

prosecution (if not, why not); and what other mechanisms are being used to address breaches of secrecy obligations (including internal disciplinary mechanisms, loss of security clearance and termination of employment).

1.31 Most of the agencies were able to provide these statistics, although the way internal investigations are described and recorded varied significantly. Broadly speaking, the responses divided incidents into 3 general categories:

i. Less serious incidents, such as accidentally leaving classified material unsecured within a workplace or self-reported minor breaches of security policy. Statistics were not sought on this category of incidents.

ii. Matters that triggered an internal investigation and either resulted in a finding of no misconduct or a decision to apply some form of administrative sanction.

iii. Matters that were reported to AFP for potential criminal investigation.

There is overlap between the last 2 categories. In the event of a serious incident, employment may be terminated (an administrative sanction) and the matter would probably also be reported to AFP for possible criminal investigation.

1.32 The number of incidents reported per agency varied. Agencies with a larger number of staff generally reported more incidents than smaller agencies.

1.33 Three agencies provided quite detailed responses that included matters such as the internal criteria used to determine which category a matter falls into. Some agencies provided case studies to illustrate the types of matters that may result in significant administrative sanctions (such as termination of employment) and the types of matters that have been reported to AFP for criminal investigation.

1.34 The available statistical information combined with the description of internal policies and the case studies suggests that, overall, administrative sanctions are the first and most common response. The types of incidents outlined in the case studies describe a class of matters that is reasonable to report to AFP. As discussed in **Chapter 10**, whether and how AFP investigates a report of a potential crime is regulated by AFP policies. Most of the matters that occurred and were reported to AFP since Part 5.6 of the *Criminal Code* commenced have been finalised without prosecution. Some matters remain active investigations.

Administrative sanctions are not always sufficient

1.35 Some agencies provided evidence to the effect that, while administrative sanctions are important, they are not always a sufficient response. In addition to the role of criminal sanctions as a proper response to actions that lead to real harm or risk of harm to national security, some agencies pointed out that administrative sanctions are of limited utility where the individual involved is no longer a Commonwealth employee. For example, no effective

administrative sanctions are available for a person who has already resigned their employment.[35] Actual case studies were provided that supported this point.

1.36 Criminal and administrative sanctions against individuals are not the only responses necessary to counter the threat of foreign interference and espionage. I note the work of the Department of Home Affairs in countering foreign interference by focusing on 'engaging those at risk', 'building resilience through risk mitigation strategies' and 'coordinating government agencies to directly defend against foreign interference activity'.[36] As the Director-General of Security noted, 'Yes, prosecutions are important … but there are other ways to efficiently and effectively reduce harm, particularly from espionage and foreign interference'.[37]

Commonwealth official

1.37 Most of the offences in Part 5.6 apply to people who obtained the relevant information by reason of being, or having been, a 'Commonwealth officer' or a person 'otherwise engaged to perform work for a Commonwealth entity'. In this report the phrase 'Commonwealth official' is sometimes used as a shorthand to describe both of these categories. However, before reviewing the offences themselves it is necessary to consider:

- Who is a Commonwealth officer?
- Who is a person otherwise engaged to perform work for a Commonwealth entity?

Commonwealth officer

1.38 Section 121.1(1) of the *Criminal Code* defines the term Commonwealth officer:

> **Commonwealth officer** means any of the following:
>
> (a) an APS employee;
>
> (b) an individual appointed or employed by the Commonwealth otherwise than under the *Public Service Act 1999*;
>
> (c) a member of the Australian Defence Force;
>
> (d) a member or special member of the Australian Federal Police;

---

35 ONI, *Submission 8*, 14. The Australian Secret Intelligence Organisation (ASIO) also noted the limited utility of administrative sanctions in relation to former employees: see ASIO, *Submission 6*, 3. This type of situation was also described by Director-General of Security: Mr Mike Burgess, Director General of Security, ASIO, *Public hearing transcript*, 25 March 2024, 17.

36 Department of Home Affairs, 'Australia's approach to countering foreign interference', *Countering Foreign Interference* (Web Page, 5 June 2023) <https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference/australias-approach>.

37 Mike Burgess, 'Director-General's Annual Threat Assessment 2024' (Speech, ASIO, 28 February 2024).

(e) an officer or employee of a Commonwealth authority;

(f) an individual who is a contracted service provider for a Commonwealth contract;

(g) an individual who is an officer or employee of a contracted service provider for a Commonwealth contract and who provides services for the purposes (whether direct or indirect) of the Commonwealth contract;

but does not include an officer or employee of, or a person engaged by, the Australian Broadcasting Corporation or the Special Broadcasting Service Corporation.[38]

1.39 Parts (a)–(e) of the definition are all people who are directly on the Commonwealth payroll. This includes all public servants, people employed under other Acts (such as under the *ASIO Act* or the *IS Act*), statutory officers and AFP and Australian Defence Force personnel. It is uncontroversial that this category of people be regarded as Commonwealth officers for the purpose of secrecy offences. It is quite appropriate to exclude those employed or engaged by the ABC or SBS from the definition of 'Commonwealth officer' for secrecy offences (but see further comments at the end of this chapter).

1.40 Paragraphs (f) and (g) of the definition of 'Commonwealth officer' relate to individuals who provide services under a Commonwealth contract, as well as those they employ to provide services (directly or indirectly) for the purpose of that contract.[39] It is reasonable that the Commonwealth would seek to bind these individuals to secrecy obligations that carry criminal penalties if they are entrusted to deal with the same sorts of information that Commonwealth employees deal with, particularly national security, defence and law enforcement related information. Contractual remedies should also be available and should be used but will not always be sufficient. It would be proper, although not strictly legally necessary, to take reasonable steps to ensure that contractors and their employees are aware of the statutory secrecy obligations that apply to them.

1.41 Bodies corporate can be subject to criminal liability in accordance with Division 12 of the *Criminal Code*.[40]

1.42 In contrast to the definition of 'Commonwealth public official' in the Dictionary of the *Criminal Code*, the definition of 'Commonwealth officer' in s 121.1(1) does not expressly

---

38 Note that many of the terms in this definition are defined either in the *Acts Interpretation Act 1901* (Cth) or in the Dictionary to the *Criminal Code* (n 32).

39 In accordance with the Dictionary to the *Criminal Code* (n 32): a *contracted services provider* means a person who is a party to a Commonwealth contract and who is responsible for the provision of services to a Commonwealth entity under the Commonwealth contract; or a subcontractor for the Commonwealth contract. *Commonwealth contract* means a contract, to which a Commonwealth entity is a party, under which services are to be, or were to be, provided to a Commonwealth entity *Services to a Commonwealth entity* includes services that consist of the provision of services to other persons in connection with the performance of the Commonwealth entity's functions.

40 Section 4B of the *Crimes Act* (n 15) enables a fine to be imposed for offences that only specify imprisonment as a penalty.

include the Governor-General, Members of either House of the Parliament, judicial officers or Ministers.

1.43 Paragraph (b) of the definition of Commonwealth officer refers to 'an individual appointed or employed by the Commonwealth otherwise than under the *Public Service Act 1999* (Cth). The Governor-General, appointed by the King as His Majesty's representative in the Commonwealth, would not fall within this definition. Nor would Members of the House of Representatives or Senators, who are 'chosen by the people' (Members and Senators who are part of the PJCIS are expressly covered by specific offences in the *IS Act*). It is unlikely that judges in their judicial capacity would fall within the definition of 'Commonwealth officer' either. This outcome is broadly consistent with the ALRC 2009 Secrecy Laws Report, which recommended that general secrecy offences focus on the executive branch of government and not extend to judicial officers acting in their judicial capacity or to Members of either House of Parliament.[41]

1.44 Ministers (including Assistant Ministers) who are part of the executive branch of government, may be in a different position. The Revised Explanatory Memorandum to the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 suggests that paragraph (b) of the definition of 'Commonwealth officer' is intended cover a Minister of State (including a Parliamentary Secretary) appointed by the Governor-General in Council under s 64 of the Constitution.[42]

---

41 Australian Law Reform Commission (ALRC), *Secrecy Laws and Open Government in Australia* (Report No 112, December 2009) [6.51] and [6.57] ('*ALRC 2009 Secrecy Laws Report*'). The ALRC recommended that the definition of 'Commonwealth officer' should include the Governor-General and ministers and parliamentary secretaries: Recommendation 6-1. The ALRC also noted that judges acting in their personal capacity (e.g. when issuing warrants) potentially fell within the meaning of 'Commonwealth officer' (under the previous definition in the *Crimes Act*) [665]. It is possible they may also fall within paragraph (b) of the definition of 'Commonwealth officer' in s 121.1 as an individual appointed (to issue warrants) by the Commonwealth, or alternatively when acting in such a capacity they may be viewed as persons 'otherwise engaged to perform work for a Commonwealth entity' for the purpose of the offences for officials.

42 National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017, Revised Explanatory Memorandum, [1251]. In *Wong v Minister for Immigration and Multicultural and Indigenous Affairs* (2004) 204 ALR 722 at 744 there is consideration of a secrecy offence in s503A of the *Migration Act 1958* (Cth) that applied to a 'Commonwealth officer' performing functions under the *Migration Act* where Commonwealth officer meant 'an individual holding office under, or employed, by the Commonwealth'). Lindgren J found that in the specific context of s 503A of *Migration Act* the provision did not apply to the Minister. However, this finding turned on the way that different parts of s503A distinguished between 'the Minister' and 'a Commonwealth officer' [89]-[99]. Lindgren J reached this conclusion without reference to the note that followed sub-s 503A(9) of the *Migration Act 1958* which said that 'a Minister is not a Commonwealth officer' [98].

Otherwise engaged to perform work for a Commonwealth entity

1.45 As the people who provide services under a Commonwealth contract and those they employ for that purpose are covered by the definition of 'Commonwealth officer', it must be assumed that the addition of the category of 'otherwise engaged to perform work for a Commonwealth entity' in each of the offences in ss 122.1, 122.2 and the offence in s 122.4 are intended to cover a different category of people.

1.46 A 'Commonwealth entity' is the Commonwealth or a 'Commonwealth authority'. A Commonwealth authority means any 'body' established under a law of the Commonwealth excluding those established under the *Corporations Act 2001* (Cth), those established under Australian Capital Territory or Northern Territory laws, bodies registered under the *Fair Work (Registered Organisations) Act 2009* (Cth) and certain Aboriginal corporations.[43]

1.47 Those who are otherwise engaged to perform *work* for a Commonwealth entity thus may include those who do that 'work' under some form of agreement or arrangement that falls short of being a contract; or those who act as an agent for a Commonwealth entity. These people may or may not be paid and their relationship with the Commonwealth is not on the same legal footing as it would be if a contract was in place, but they are nevertheless potentially covered by the offences. It not completely clear whether the concept of 'engaged to perform *work*' in the way that phrase is used in Part 5.6 is intended to include people who are engaged to perform 'services'; however, there is a reasonable argument that it does. The term 'work' in this context seems to be being used as a verb and is clearly not limited to employment or contract service providers (because both are already covered by the definition of 'Commonwealth official'). Thus, to give 'work' meaning in this phrase it must be being used in a wider sense such as that in the Macquarie Dictionary (online) 'to effect, accomplish, cause or do'. Engaged to perform work in this context therefore likely includes engaged in some way outside of an ordinary contract or sub-contract to perform services for a Commonwealth entity.

1.48 The ALRC 2009 Secrecy Laws Report concluded that, in the context of the wider public sector, imposing a secrecy offence on persons who are not otherwise Commonwealth officers required more than an agreement or arrangement to justify the imposition of criminal liability. In the context of intelligence agencies, ALRC accepted that an 'agreement or arrangement' may be sufficient to impose criminal liability, provided that the individual was made aware of the sensitive nature of the information involved and the implications of unauthorised disclosure.[44]

---

43 *Criminal Code* (n 32) Dictionary. Additional exclusions from the definition can be made by regulation, but there are currently no exclusions in the *Criminal Code Regulations 2019*.

44 *ALRC 2009 Secrecy Laws Report* (n 41) 190-1 [6.28]-[6.29].

1.49 The *IS Act, ONI Act* and *ASIO Act* expressly seek to capture individuals who have an 'agreement or arrangement' short of a contract or employment relationship within the scope of secrecy offences in those Acts. Agencies operating under the *IS Act* gave evidence to this review that it is their practice to have those that they have an 'agreement or arrangement' with sign a document indicating they understand the secrecy obligations that apply to them.

1.50 There is a possible anomaly in the way ABC and SBS staff and contractors are treated. As noted above, ABC and SBS staff and contractors are expressly excluded from the definition of 'Commonwealth officer'. However, the ABC and SBS are both established under relevant laws of the Commonwealth and are Commonwealth entities.[45] Therefore, those who are engaged to perform work for them would seem to fall into the category of people who are 'otherwise engaged to perform work for a Commonwealth entity' and thus fall within the scope of the offences in ss 122.1, 122.2 and 122.4. It seems unlikely that this was the policy intention, and the matter could easily be put beyond doubt by excluding ABC and SBS from the definition of a 'Commonwealth entity' using the regulation making power or by an amendment to the *Criminal Code*.

45 *Australian Broadcasting Corporation Act 1983* (Cth) s 5; *Special Broadcasting Service Act 1991* (Cth) s 5.

Chapter 2: Secrecy and threats to national security

2.1 In accordance with the *INSLM Act* I must consider whether the provisions in Part 5.6 of the *Criminal Code* remain necessary and proportionate to any threat of terrorism or threat to national security or both.[46] To perform this assessment I must examine the current threat landscape as well as that which predicated the introduction of the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth) (*EFI Act*).

2.2 This chapter considers evidence on the threat to national security posed by the disclosure of certain information – particularly evidence from the Australian Security Intelligence Organisation (ASIO) about the current threat of foreign interference and espionage. The chapter also summarises evidence, particularly from media and civil society groups, about the threat secrecy laws can pose to a free press and how this threat can undermine national security by undermining an essential part of our democracy. Lastly, the chapter discusses the threat posed by what is known as the 'mosaic effect' and how it fits (or does not fit) with ordinary principles of criminal law.

Threats from espionage and foreign interference

2.3 ASIO provided this review with the following overview of the current threat of espionage and foreign interference:

> The security threats facing Australia are more sophisticated than ever before, with espionage occurring at a scale and scope that is targeting all levels of government, and across defence to steal classified and sensitive information.
>
> Foreign powers, particularly those with sophisticated intelligence services, use a variety of complex means to aggressively seek to steal secrets about Australia's military capabilities, government decision-making, foreign policy, critical infrastructure, sensitive research and innovation, and personal information, especially bulk data.
>
> This includes through the targeting of Australian Government security clearance holders with access to such classified and sensitive government information. For example, since the announcement of AUKUS, there has been a marked increase in the targeting of people working in Australia's defence industry.
>
> Foreign intelligence services are also actively trying to recruit Australian insiders (current and former employees or contractors who enjoy legitimate access to information, techniques,

46 *Independent National Security Legislation Monitor Act 2010* (Cth) s 6(1)(b)(ii)-(iii) ('*INSLM Act*'); *Criminal Code Act 1995* (Cth) ('*Criminal Code*').

activities, technology, assets or facilities) with access to personal information to enable foreign interference, including to help repress critics of overseas regimes.

Given these activities are designed to be inherently clandestine, it is not always possible to attribute the activities of insiders compromising sensitive material to a foreign power. In sophisticated cases, the spies use agents or proxies to hide the connection to a foreign government.

In addition, there are insiders who disclose and deal with government information without authorisation, whether intentionally or unintentionally. For example, an insider could intentionally disclose classified or privileged information as an act of revenge, or unintentionally reveal privileged information to a third-party.

Regardless of the intent, the unauthorised use and disclosure of national security classified information raises risks to security. It puts this information at risk of being obtained by hostile actors – either directly through the actions of insiders, or by the insider removing the material from government protection, which in turn makes the information potentially vulnerable to exploitation by hostile foreign entities.

This means that even in cases that appear not to directly relate to espionage or foreign interference, in the current threat environment, there are still relevant espionage and foreign interference risks that need to be considered.[47]

2.4 The Director-General of Security, Mr Mike Burgess, reiterated many of the same points in his opening statement at the public hearings held to inform this review. Mr Burgess said that the unauthorised disclosure of sensitive information 'could undermine Australia's national security, sovereignty and economic prosperity and potentially pose a threat to life'.[48]

2.5 The threat of espionage and foreign interference described by ASIO is a continuation of the threat described at the time the *EFI Act* was introduced. In 2018 the threat of espionage and foreign interference was described as an 'unprecedented' challenge 'posing a grave threat to Australia's sovereignty, prosperity and national security'.[49] The offences in Part 5.6 were intended to play a role in responding to this threat. For example, the offences were described as being necessary to create a deterrent against foreign adversaries who seek to exploit weaknesses in information protection frameworks, as well as public officials who inadvertently or otherwise create those weaknesses through unauthorised disclosures.[50]

47 Australian Security Intelligence Organisation (ASIO), *Submission 6*, 4.

48 Mr Mike Burgess, Director-General of Security, *Public hearing transcript*, 25 March 2024, 10.

49 Explanatory Memorandum, National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2018, 11 [40].

50 Evidence to the Parliamentary Joint Committee on Intelligence and Security (PJCIS), Parliament of Australia, Canberra, 16 March 2018, 33-35 (Mr Duncan Lewis, former Director-General of Security).

Stricter secrecy offences were also described as providing a 'strong prosecutorial option' where the link to a foreign principal – and therefore espionage and foreign interference offences – could not be proved (but may exist).[51]

2.6 I accept that Australia faces a significant and persistent threat of espionage and foreign interference. One aspect of this threat relates to ongoing efforts by foreign actors to acquire sensitive information from individuals who knowingly, or otherwise, reveal this sought-after information.

2.7 In my view, the threats that ASIO describes relate most directly to the espionage, foreign interference and sabotage offences contained in Part 5.2 and Division 82 of Chapter 5 of the *Criminal Code*. A key difference between these offences and those in Part 5.6 is the active and direct involvement of a foreign principal. However, I also acknowledge ASIO's advice that, given the actions of foreign intelligence services are inherently clandestine, it is not always possible to attribute the activities to a foreign power.[52] There is also the risk that a person acting for reasons entirely unrelated to espionage or foreign interference may nevertheless unwittingly provide, or risk providing, foreign actors or criminals with critical information contrary to the national interest. This is a circumstance where the Part 5.6 offences are particularly relevant.

Threats where there is no apparent link to a foreign principal

2.8 The following well-publicised cases provide examples of matters where there is no apparent link to a foreign principal and therefore the conduct is unlikely to fall within the scope of foreign interference or espionage offences. The relevant conduct in each of these cases occurred before Part 5.6 was enacted, but if they occurred today each could potentially be investigated and possibly prosecuted under that Part:

- In 2017 the ABC published a series of stories known as 'the Afghan Files'. The stories raised allegations of the killing of civilians in Afghanistan by members of the Australian Defence Force (ADF). The ABC said it relied upon classified documents that had been leaked to it by informants. The Australian Federal Police (AFP) investigated the matter, and this led to former ADF lawyer Mr David McBride being convicted of theft of Commonwealth property and unlawfully communicating

51 PJCIS, Parliament of Australia, *Advisory Report on the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (Report, June 2018) 101 ('*PJCIS EFI Bill Report*').

52 ASIO, *Submission 6*, 4.

military information.[53] There was no evidence to suggest Mr McBride acted to intentionally aid a foreign power. Nevertheless the judge found that disclosure of some of the documents (particularly the 'rules of engagement') would, or would have been likely to, have prejudiced the defence, national security or international relations of Australia.[54] Mr McBride's motives for disclosing the documents did not include seeking to disclose potential war crimes.[55]

- In 2018 the *Sunday Telegraph* published a story, written by Ms Annika Smethurst, about proposed amendments to the powers of the Australian Signals Directorate (ASD). The story included an image of part of a security classified document. On 4 June 2019, while investigating possible offences arising from this story, AFP searched Ms Smethurst's residence. Ms Smethurst successfully challenged the validity of the search warrant in the High Court of Australia.[56] There was no suggestion that the disclosure of the proposed changes to ASD's powers and functions was at the behest of a foreign power.
- Mr Alan Johns (a pseudonym) was subject to revocation of his security clearance. In complaining to an agency about the revocation of his security clearance and what he perceived as unfair treatment, he disclosed sensitive information on an unsecured platform.[57] He was subsequently prosecuted. The judge accepted that Mr Johns was not intending to deliberately harm Australia's national security interests or to pass material to third parties but said that his conduct did pose risks with potentially serious consequences.[58] Mr Johns pleaded guilty to 5 charges based on his treatment of sensitive information over a number of months and was sentenced to a term of imprisonment.[59]
- The prosecution of Mr Bernard Collaery (which was ultimately dropped) and 'Witness K' (who pleaded guilty) concerned the disclosure of information about an

53 *R v McBride (No 4)* [2024] ACTSC 147 ('*R v McBride*').

54 *R v McBride* (n 53) [116], [125]-[126], [193]. The judge also accepted that disclosure of the identities of any Special Operations Command or Special Forces personnel may have exposed them to exploitation by foreign intelligence services and that while there is no evidence that this has occurred it is an ongoing concern to the Australian Defence Force [124].

55 *R v Mc Bride* (n 53) [101], [163]-[168].

56 *Smethurst v Commissioner of Police* (2020) 272 CLR 177. No charges were laid against Ms Smethurst. The Australian Federal Police (AFP) conducted a review on their handling of sensitive investigations following this case. It resulted in the introduction of new *AFP National Guideline on Sensitive Investigations* that applies to investigations involving journalists. It also precipitated a Ministerial Direction to AFP relating to the investigation of journalists. Both outcomes are discussed in Chapter 4.

57 Grant Donaldson, INSLM (former), *The Operation of Part 3, Division 1 of the National Security Information (Criminal and Civil Proceedings) Act 2004 as it applies in the Alan Johns matter* (Report, 17 June 2022) 9.

58 *R v Johns (a pseudonym) (No 2)* [2023] ACTSC 83, [14].

59 *R v Johns (a pseudonym)* [2019] ACTSC 399.

alleged Australian intelligence operation in Timor-Leste to collect information in the context of treaty negotiations.[60] Both were charged with secrecy offences but not espionage.

2.9 It is notable that 2 of these cases directly involve journalists and one a lawyer. The secrecy offences in Part 5.6 of the *Criminal Code* apply to a wide range of individuals involved with government, whether they involve themselves formally in the course of employment or contracting or otherwise undertake work for government (see **Chapter 1**). There are also specific offences targeted at people who are not, and have never been, connected to government, including journalists (see **Chapter 8**).

Threats to a free press, accountability and trust in government

2.10 In considering the proportionality of secrecy offences, it is necessary to consider not only the threat they are expressly directed towards (including preventing foreign actors or others gaining access to information that could harm critical national interests) but also harms that may arise because of the breadth and scope of the offences themselves – for example, threats to the rule of law and threats to the institutions that support our democracy, including a free press.

2.11 It is a longstanding principle that the public should have access to information about their government unless there is a compelling reason to protect it. The principle applies beyond the minimum requirement of the implied freedom of political communication (see **Chapter 3**) and is reflected in a range of laws, including the *Administrative Decisions (Judicial Review) Act 1977* (Cth), the *Freedom of Information Act 1982* (Cth) (*FOI Act*), the *Archives Act 1983* (Cth) and the *Privacy Act 1988* (Cth), as well as in the way courts assess public interest immunity claims.[61]

2.12 The role of a free press is widely accepted as an important part of a properly functioning democracy. In the specific context of secrecy offences, there have been government

60 *R v Collaery (No 12)* [2022] ACTSC 108.

61 Maureen Henninger, 'Reforms to Counter a Culture of Secrecy: Open Government in Australia' (2018) 35(3) *Government Information Quarterly* 398; Daniel Stewart, 'Simplifying Government Secrecy?' in Ron Levy, Molly O'Brien, Simon Rice, Pauline Ridge, Margaret Thornton (eds), *New Directions for Law in Australia: Essays in Contemporary Law Reform* (ANU Press, 2017) 449, 451; Kylie Weston-Scheuber, 'Hear No Evil, See No Evil, Speak No Evil: The Secretisation of Information by Government in Australia' (2022) 34(1) *Bond Law Review* 31, 32; Justice Susan Kenny, 'Secrecy Provisions: Policy and Practice' (Speech, National Information Law Conference, 24 March 2011) 2–3; *Commonwealth of Australia v Fairfax & Sons Limited* (1980) 147 CLR 39.

directions and policy statements about the need to consider the role of public interest journalism. The Attorney-General has directed the AFP to 'take into account the importance of a free and open press in Australia's democratic society' when investigating journalists.[62] The recent Attorney-General's Department (AGD) *Review of Secrecy Provisions* recommended that defences should be considered when framing secrecy offences, including to protect public interest journalism.[63]

2.13 The Alliance for Journalists' Freedom (AJF) said that citizens rely on the press to make informed decisions about their government:

> Citizens rely on information about the operations of government and about elected representatives to cast their votes. Matters of national security are of particular concern to voters. Citizens gain information about government policies and actions through media reporting. To report openly and honestly about the government and, consequently, to hold the government to account, journalists must be able to carry out their work, including investigative reporting, in a free and safe manner and within limits that are carefully drawn so as not to be excessively restrictive.[64]

2.14 It is also the case that at times 'media scrutiny makes our government, and its agencies work better' by bringing misconduct or mismanagement to light and instigating change.[65] The Robodebt matter, the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry and allegations about war crimes in Afghanistan were all mentioned as examples during this review.

2.15 The Media, Entertainment and Arts Alliance (MEAA) said that the Part 5.6 offences 'and the hundreds of other secrecy clauses across federal legislation – undermine the public's right to know' and were designed to shut down scrutiny:

> In Australia, public interest journalism is under threat. The existence of Part 5.6 has severely curbed the legitimate work of journalists. This legislation, with its broad definitions, is deliberately designed to shut down legitimate media inquiry.[66]

2.16 Australia's Right to Know (ARTK) submitted that it should be the role of government, not the role of the media and the public, to justify why something should not be public:

---

62 Attorney-General (Cth), *Ministerial Direction (Australian Federal Police): Australian Federal Police Act 1979*, 20 October 2023.

63 Attorney-General's Department (AGD), *Review of Secrecy Provisions* (Final Report, 21 November 2023) 8 [18], 29 [113].

64 Alliance for Journalists' Freedom (AJF), *Submission 11*, [1.7]–[1.8].

65 Mr Peter Greste, AJF, *Public hearing transcript*, 26 March 2024, 115–116.

66 Media, Entertainment and Arts Alliance (MEAA), *Submission 9*, 1.

> Ultimately, it should not be for the media or the public to justify why the public should be able to receive information about its own government free from the risk of criminal sanction. It should instead be for government to justify – clearly and unambiguously – why the public should not receive information about its own government and why the threat of criminal sanction is the only appropriate mechanism to stop the public receiving that information.[67]

2.17 Expert academics in the field submitted that media organisations' ability to report on matters of public interest has a number of benefits, including to protect freedom of expression in line with Australia's international obligations and also to ensure transparency, accountability and compliance with the rule of law.[68]

2.18 Secrecy offences are not the only legislative processes impacting on the operation of a free press. Though outside the scope of this review, the MEAA noted that the operation of freedom of information laws and defamation laws and the operation of whistleblower provisions also have a disproportionate impact on the media in Australia.[69]

2.19 The cumulative effect of provisions that hamper the activities of a free and open press is described as the 'chilling effect'. AJF noted that 'the potential for criminal sanctions in circumstances where there has been no actual harm has a chilling effect on the willingness and ability of Commonwealth officers to disclose information to journalists or civil society members that is in the public interest'.[70] At the public hearing, MEAA, ARTK and the joint academic group agreed that the chilling effect has a real impact on journalistic practice.[71] The MEAA noted:

> one particular instance post the introduction of these offences where just simply trying to embark on the process of normal story gathering or the normal journalistic process and trying to gather information about a particular national security issue was so complex and difficult to navigate that it ultimately scared off a prospective source because simply having basic communications with that particular person raised the risk of … committing an offence …[72]

---

67 Australia's Right to Know (ARTK), *Submission 12*, 5.

68 Joint Academic Submission, *Submission 13*, 12.

69 MEAA, *Submission 9*, 3. Other submitters, including the Human Rights Law Centre (HRLC) and AJF made similar points, especially in relation to whistle-blowers: see Mr Peter Greste, AJF, *Public hearing transcript*, 26 March 2024, 115–116; HRLC, *Submission 14*, 7.

70 AJF, *Submission 11*, [6].

71 Dr Kieran Hardy, Griffith University, *Public hearing transcript*, 25 March 2024, 52; Ms Rebecca Ananian-Welsh, University of Queensland, *Public hearing transcript*, 25 March 2024, 52; Mr Robert Todd, ARTK, *Public hearing transcript*, 26 March 2024, 125–126.

72 Mr Paul Farrell, MEAA, *Public hearing transcript*, 26 March 2024, 120.

2.20 Reporters without Borders recently ranked Australia 39th out of 180 countries for press freedom in 2024, down from 27th in 2023. One of the reasons given for this ranking is Australia's national security laws.[73]

2.21 Civil Liberties Australia highlighted 'historically low trust in government' and the role excessive secrecy has in undermining trust.[74] Other submitters also recognised this risk.[75]

2.22 It is important to acknowledge that even the Director-General of Security, who is tasked with managing some of the Commonwealth's most sensitive operations, including counterterrorism and foreign interference matters, clearly recognises that transparency and accountability – including some public scrutiny – are important aspects of the work of national security agencies. At the public hearing the Director-General of Security said, 'I strongly believe that appropriate oversight and accountability are critical, and I continue to promote transparency'.[76]

2.23 Threats to a free press, which limit the disclosure of misconduct or wrongdoing and the scrutiny and accountability of government that goes with it, are also threats that need to be considered when examining secrecy laws. Public scrutiny and protecting essential interests are not mutually exclusive, but some secrecy is always going to be required and this will always have implications for the legitimate activities of the press and others. The challenge lies in ensuring an appropriate legal framework that both supports the legitimate activities of the media and civil society groups as an essential element of our democracy, and protects Australia's national security and other essential interests from espionage, foreign interference and other threats.

2.24 Australia's international law obligations on freedom of expression and the implied freedom of political communication are discussed further in **Chapter 3**. The offences (and defences) that apply to journalists and other non-officials are discussed in **Chapters 8**–**9**. Journalists rely on sources. In this context, those sources will almost always be current or former Commonwealth officials subject to the offences discussed in **Chapters 4**–**7**. There are also other legal regimes outside the scope of this review – for example, the *Public Interest Disclosure Act 2013* (Cth) and the *FOI Act* – that are relevant to sources of information for journalists.

---

73 Reporters Without Borders, 'Australia' (Web Page) <https://rsf.org/en/country/australia>.

74 Civil Liberties Australia, *Submission 1*, 1–2.

75 Dr Kieran Hardy, Griffith University, *Public hearing transcript*, 25 March 2024, 48.

76 Mr Mike Burgess, Director-General of Security, ASIO, Public hearing transcript, 25 March 2024, 10.

Threats from the mosaic effect

2.25 When considering the harms that can result from the unauthorised disclosure of national security information, numerous submissions – particularly those from National Intelligence Community agencies – make reference to the 'mosaic effect'. To provide background and context to later chapters, I will summarise here what the 'mosaic effect' is and why it does not fit easily with ordinary principles of criminal culpability.

2.26 Most judicial consideration of the concept of the 'mosaic effect' has been in public interest immunity (PII) cases. In *Watson v AWB Ltd (No 2)*, Justice Foster adopted the Director-General of Security's description of 'mosaic analysis':

> Mosaic analysis involves combining pieces of information to enable a 'picture' to emerge from which inferences can be drawn by targets, or other persons of interest, about matters not otherwise known to them. Some of the pieces of information may appear to be disparate and/or benign; and specific (but important) items of information may only be known by the target(s) or other persons of interest (making it difficult to precisely assess the risk posed by mosaic analysis in any particular scenario).[77]

2.27 This description has been referred to in a number of subsequent PII cases.[78]

2.28 In this review ASD submitted:

> information which may appear innocuous could, when viewed in aggregate and alongside publicly available information, be used by foreign intelligence services to gain access to or disrupt ASD business or reveal the details of covert targets, capability or methods used by ASD. An individual could also communicate harmful ASD information without knowing or believing it to be harmful.[79]

2.29 Other agencies made submissions to the same effect.[80]

2.30 I accept that the unauthorised disclosure of some types of information enlivens the 'mosaic effect' and can be a real threat to national security. However, I also consider that any reference to it in a criminal context must be compatible with the rule of law and principles of criminal culpability.

2.31 Criminal offences have both a physical element (an effect) and a harm element (a mental component) – that is, to create a criminal offence, there must ordinarily be both an effect (the physical element, usually a harm or risk of harm) and a mental element (usually

---

77 *Watson v AWB Ltd (No 2)* (2009) 259 ALR 524, [32].

78 See, eg, *Australian Securities and Investments Commission v P Dawson Nominees Pty Ltd (No 5)* [2010] FCA 232, [11]–[12] and *Australian Securities and Investments Commission v P Dawson Nominees Pty Ltd* [2009] FCAFC 183, [56]–[63].

79 Australian Signals Directorate, *Submission 4*, 5.

80 Office of National Intelligence, *Submission 8*, 2; Australian Criminal Intelligence Commission, *Submission 16*, 3–4; AFP, *Submission 18*, 9.

recklessness to that harm). In contrast, PII cases only require establishment of the physical element (harm or risk of harm). Furthermore, in PII cases the disclosure of information (including in reliance on a 'mosaic effect' argument) will only be ordered where a court determines that the public interest in non-disclosure outweighs the public interest in disclosure. Therefore, a concept like the 'mosaic effect' cannot easily be taken from PII cases and applied directly in criminal law.

2.32 The Human Rights Law Centre noted that the mosaic effect does not accord with ordinary criminal law principles because 'the discloser cannot intend or know the actions of an unknown hypothetical third party, and they should not be responsible for the third parties actions'.[81]

2.33 The Law Council of Australia supported this view. It said:

> It is fundamental to the main purpose of criminal law to deter and punish, that entails criminal offences that focus on the concept of individual culpability and establishing as an element of the offence the criminal intention for one's actions.[82]

2.34 AGD considered that, while it may, in practice, be challenging to prove the mental element of an offence (recklessness) when the physical element (harm) depends on the 'mosaic effect', this will not always be the case:

> It may, in practice, be more challenging to prove a defendant's awareness of a substantial risk of harm in cases where that harm is dependent on the 'mosaic effect', though this will not necessarily be the case – for example, there may be evidence based on a defendant's expertise and experience as an officer with a demonstrated understanding of the effect of combining different pieces of information.[83]

2.35 The knowledge of 'insiders', particularly those who work in intelligence agencies and are familiar with the 'mosaic effect', may mean that it is both reasonable and possible to establish the mental element of an offence taking their training and experience into account. However, that is not the case for those without that background. This issue was considered by former INSLM the Hon. Roger Gyles AO KC in his review of the impact of s 35P of the *Australian Security Intelligence Organisation Act 1979* (Cth) in 2016:

> It may be accepted that information about an [ASIO Special Intelligence Operation (SIO)] may seem innocuous, but may be significant if combined with other information that is known: the 'mosaic effect'. That does not deny that some information about an SIO will have no, or

81 HRLC, *Submission 14*, 6.

82 Law Council of Australia, *Submission 19*, 12.

83 AGD, *Submission 7*, 6. AGD goes on to say that the presence of security markings (like 'secret' or 'top secret') on documents can assist in establishing a defendant's reckless to the harm – this is discussed further in Chapter 4.

> no continuing, operational significance. It is one thing to enforce an implication of harm in relation to insiders bound by a duty of confidence and with knowledge (or the means of knowledge) about an SIO. It is quite another to apply that implication to third parties who are not so bound and who do not have such knowledge.[84]

2.36 This view was echoed more generally by AFP. It noted that, while it was difficult to reconcile the principles of criminal responsibility with the mosaic effect when dealing with outsiders, the risk of disclosure of information – including the potential harm and understanding of the mosaic effect – would be 'quite apparent to officers who have thorough security awareness training and regularly handle sensitive material'.[85]

2.37 There is further discussion of the mental element of recklessness in **Chapter 4**.

84 Roger Gyles, INSLM (former), *Report on the Impact on Journalists of Section 35P of the ASIO Act* (Report, October 2015) 22 [41].

85 AFP, *Submission 18*, 6.

Chapter 3: Human rights, international obligations and constitutional considerations

3.1 Section 8 of the *INSLM Act* requires that when conducting a review I must have regard to Australia's obligations under international agreements.

3.2 This chapter discusses Australia's obligations in relation to 'freedom of expression' in art 19(2) of the *International Covenant on Civil and Political Rights* (ICCPR). Article 19(2) is relevant to all of the offences in Part 5.6. In addition, art 14(2) of the ICCPR contains a right to be presumed innocent until proven guilty according to law. This right is particularly relevant to defences and is discussed in **Chapter 9** rather than here.

3.3 Consideration of Australia's human rights obligations at every stage of the development of law and policy is a key element of the Australian Human Rights Framework.[86] However, human rights obligations are not the only type of international obligations that must be considered. In the context of secrecy offences, Australia's obligations under a range of international agreements about sharing and protecting classified information are also relevant and are discussed in this chapter.

3.4 Of course, all Commonwealth laws must be consistent with the Constitution. The implied freedom of political communication is particularly relevant to the deemed harm offence (**Chapter 4**), proposed general secrecy offence (**Chapter 7**) and offences that apply to non-officials (**Chapter 8**). This review does not seek to reach any concluded view on constitutional issues. However, a brief overview of the implied freedom of political communication is provided in this chapter to inform discussion about the limits of those offences.

Article 19: the right to 'freedom of expression'

3.5 The right to freedom of opinion and expression is contained in art 19 of the ICCPR. Article 19(2) provides:

> Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his [or her] choice.

86 Australian Human Rights Commission (AHRC), *Revitalising Australia's Commitment to Human Rights: Free & Equal Final Report 2023* (Final Report, 8 November 2023) 54.

3.6 The United Nations Human Rights Committee (UNHRC) has observed that this right is a foundational right in democracies:

> [The right to freedom of opinion and expression] constitute[s] the foundation stone for every free and democratic society. The two freedoms are closely related, with freedom of expression providing the vehicle for the exchange and development of opinions.[87]

3.7 The UNHRC has also emphasised the role of the media in freedom of expression:

> a free, uncensored and unhindered press or other media is essential in any society to ensure freedom of opinion and expression… The free communication of information and ideas about public and political issues between citizens, candidates and elected representatives is essential. This implies a free press and other media able to comment on public issues without censorship or restraint and to inform public opinion.[88]
>
> … the penalisation of a media outlet, publishers or journalist solely for being critical of the government or the political social system espoused by the government can never be considered to be a necessary restriction of freedom of expression.[89]

3.8 The secrecy offences in Part 5.6 limit free communication and a free press. This therefore requires consideration of Australia's obligations under art 19. Article 19 is not an absolute right, it can be restricted in accordance with art 19(3).

Freedom of expression is not unlimited

3.9 Article 19(3) provides for restrictions to be 'provided by law' including when 'necessary … for the protection of national security or of public order'.

3.10 The Australian Human Rights Commission (AHRC) explained that this means limitations to the right to freedom of expression must be:

- *provided by law* — laws limiting the right must be made accessible to the public and must provide sufficient guidance to both those executing the laws and those whose conduct is being regulated
- *necessary and proportionate* — to achieve a permissible purpose. At the very least, the law must restrict the right only to the absolute minimum degree necessary to achieve the legitimate purpose for the law.[90]

---

87 See United Nations Human Rights Committee (UNHRC), *General Comment No. 34 on Article 19: Freedoms of Opinion and* Expression, 102nd sess, UN Doc CCPR/C/GC/34 (12 September 2011) ('*UN General Comment 34*'). The views of the UNHRC are not binding but are considered persuasive.

88 *UN General Comment 34* (n 87) [13].

89 *UN General Comment 34* (n 87) [42].

90 AHRC, *Submission 17*, 8.

Provided by law

3.11 The requirement that restrictions be 'provided by law' might not be satisfied by obligations that are imposed through policies that the executive can change at any time.[91] At the public hearing the Australian Human Rights Commissioner said:

> in addition to being necessary and proportionate, the requirement under article 19 is that, of course, any restrictions be made by law. And one of the difficulties in terms of having a policy document that is changeable and that can be changed without full parliamentary oversight and without that level of transparency and accountability, is you do call into question that fundamental requirement of being made by law, which, as we've mentioned, really does highlight the interrelationship between freedom of expression and the rule of law as human rights obligations.[92]

3.12 Ms Jane Fraser, AHRC Senior Lawyer, elaborated:

> things that limit the right must be accessible to the public and must provide sufficient guidance both to those executing the laws and those whose conduct is being regulated. So the limitations need to be as provided by law.[93]

3.13 This is particularly relevant to the offence in s 122.1 of the *Criminal Code*, where essential elements of the offence are determined by a classification decision made in accordance with a 'policy framework'. It is also relevant to offences that depend on whether something is connected to the functions of the Defence Intelligence Organisation (DIO). The DIO's functions are not set out in law, so they can be altered without parliamentary involvement (these issues are discussed further in **Chapter 4**).

Necessary and proportionate

3.14 Restrictions on the freedom of communication must be 'necessary' for a legitimate purpose and must not be 'overbroad'. As to the latter, restrictive measures must:

- conform to the principle of proportionality
- be appropriate to achieve their protective function
- be the least intrusive instrument amongst those which might achieve their protective function
- be proportionate to the interest to be protected.[94]

---

91 AHRC, *Submission 17*, 16 [57]; *UN General Comment 34* (n 87) 6–7 [25].
92 Ms Lorraine Finlay, Human Rights Commissioner, AHRC, *Public hearing transcript*, 25 March 2024, 33.
93 Ms Jane Fraser, AHRC, *Public hearing transcript*, 25 March 2024, 33.
94 *UN General Comment 34* (n 87) [33]–[34].

3.15 The justifiable restriction on freedom of expression on the ground of national security is usually described as being narrow: this ground of restriction is invoked when the political independence or the territorial integrity of the State is at risk.[95] Key commentators have noted that 'many governments have, however, a tendency to invoke protection of national security to justify far-reaching restrictions on freedom of expression of opposition groups, politicians and critical media' and that these have been found to be violations of art 19 of the ICCPR.[96]

3.16 The UNHRC *General Comment No. 34 on Article 19: Freedoms of Opinion and Expression* warns against laws that supress information that does not actually harm national security:

> Extreme care must be taken by States parties to ensure that treason laws and similar provisions relating to national security, whether described as official secrets or sedition laws or otherwise, are crafted and applied in a manner that conforms to the strict requirements of paragraph 3. It is not compatible with paragraph 3, for instance, to invoke such laws to suppress or withhold from the public information of legitimate public interest that does not harm national security or to prosecute journalists, researchers, environmental activists, human rights defenders, or others, for having disseminated such information.[97]

3.17 Accordingly, a key question for consideration is whether the restrictions on freedom of expression imposed by the offences in Part 5.6 of the *Criminal Code* are 'necessary' for the protection of national security or public order as understood in the context of the UNHRC's comments. This includes the requirement that laws not penalise the publication of information that does not harm national security or public order nor penalise journalists and others who disseminate this type of information.

3.18 Consistent with this, the AHRC submitted that offences should be harm-based and confined to essential public interests (this is also discussed in **Chapters 4** and **5**).[98] AHRC said this is particularly so for offences that apply to non-officials (see **Chapter 8**).[99] On the proposed new

---

95 Sarah Joseph and Melissa Castan, *The International Covenant on Civil and Political Rights: Cases, Material and Commentary* (3rd ed, 2013) 612, citing United Nations Commission on Human Rights, *Siracusa Principles of the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, 41st sess, Agenda Item 18, UN Doc E/CN.4/1985/4 (28 September 1984) 6.

96 Manfred Nowak, *UN Covenant on Civil and Political Rights: CCPR Commentary* (NP Engel Publishing, 2nd ed, 2005) 464.

97 *UN General Comment 34* (n 87) [30].

98 AHRC, *Submission 17*, 12–14.

99 AHRC, *Submission 17*, 12 [42]. Article 10 of the *European Convention for the Protection of Human Rights and Fundamental Freedoms* contains a provision similar to art 19 of the ICCPR. In a case that considered art 10 in the context of a former member of the security service of the United Kingdom, the House of Lords found that the 'special position' of such a person permitted broader restrictions, at least in a context where there were sufficient safeguards and avenues for authorised disclosures: *R v Shayler* [2002] UKHL 11.

general offence, AHRC agreed with an earlier ALRC finding that 'to warrant a criminal penalty, disclosures must harm more than the effective working of government or commercial or personal interests'.[100] While it doubted that a general offence was needed, AHRC said that, if one was enacted, it should be limited to specific identifiable harms to an essential public interest (see **Chapter 7**).[101]

3.19 To comply with art 19 of the ICCPR, laws limiting freedom of expression need to be tailored as narrowly as possible to the identified harm to national security or public order. AHRC submitted 'that criminalising all information made or obtained in connection with a domestic intelligence agency's functions is neither necessary or proportionate to achieve the legitimate objective of national security'.[102] I explore this proposition in detail in **Chapter 4**.

3.20 In its first consideration of the National Security Amendment (Espionage and Foreign Interference) Bill 2017 (EFI Bill), the Parliamentary Joint Committee on Human Rights (PJCHR) asked the then Attorney-General to respond to questions on whether the measures in the Bill were 'rationally connected' to the stated objectives of the Bill and whether the limitation of the right to freedom of expression was reasonable and proportionate to achieve the objectives of the Bill.[103] The then Attorney-General subsequently proposed a number of amendments, and the PJCHR summarised the effect of the proposed amendments in its next report:

> Broadly, the amendments aim to narrow the scope of some key definitions and the offences that relate to non-Commonwealth officers; remove strict liability from some offences; and to strengthen the defence for journalists. …, some of these amendments are likely to assist with the proportionality of the limitation on the right to freedom of expression.[104]

3.21 In considering these proposed amendments, as well as the secrecy offence provisions and the right to freedom of expression, the PJCHR concluded:

> While there have been some amendments to the proposed secrecy offences which address a number of concerns, some concerns as to the proportionality of the limitation on the right to freedom of expression remain. The combination of elements means there is a risk that the offences as drafted are overly broad and may inappropriately restrict a range of

100 AHRC, *Submission 17*, 19 [73].
101 AHRC, *Submission 17*, 19–20.
102 AHRC, *Submission 17*, 14 [50].
103 Parliamentary Joint Committee on Human Rights (PJCHR), *Human Rights Scrutiny Report* (Report No 2, 13 February 2018) [1.37] ('*PJCHR Human Rights Scrutiny Report 2*').
104 PJCHR, *Human Rights Scrutiny Report* (Report No 3, 27 March 2018) [2.293] ('*PJCHR Human Rights Scrutiny Report 3*').

> communications and conduct beyond what is necessary to achieve the stated objective of the measure.[105]

In its response, the PJCHR also noted that the then Attorney-General had flagged potential additional amendments to strengthen safeguards and indicated that those types of amendments could further address concerns on the proportionality on the limits on the right to freedom of expression.[106]

3.22 Since the PJCHR's report, the effect of some of the offences has been expanded by changes to other legislation, including expansion of agency functions under the *Intelligence Services Act 2001* (Cth), the *Office of National Intelligence Act 2018* (Cth) and the *Australian Security Intelligence Organisation Act 1979* (Cth) (also see **Chapter 4**).

International agreements about protecting information

3.23 As noted in the introduction to this chapter, international human rights obligations are not the only relevant international obligations in the context of secrecy offences. In its submission to this review the Office of National Intelligence noted:

> Australia is also party to a number of international agreements with Treaty status concerning the protection of partner information …[107]

3.24 Australia is party to several of these types of agreements.[108] The basic framework of each is broadly similar. The *Agreement between the Government of Australia and the Government of the United States of America concerning security measures for the protection of classified information*[109] is a good example. It sets out a number of mutual conditions relating to the access and handling of classified information. Most of these are administrative in nature and go to how information is to be stored and transmitted. There is a general commitment that

105 *PJCHR Human Rights Scrutiny Report 3* (n 104) [2.325].

106 *PJCHR Human Rights Scrutiny Report 3* (n 104) [2.329].

107 Office of National Intelligence (ONI), *Submission 8*, 15. ONI did not provide any specific examples or make additional submissions on this point.

108 These include *Exchange of Notes constituting an Agreement between the Government of Australia and the Government of the Federal Republic of Germany for the Reciprocal Safeguarding of Classified Material*[1979] ATS 20 (signed and entered into force 27 November 1979); *Agreement between the Government of Australia and the Government of Canada concerning the Protection of Defence Related Information exchanged Between Them* [1996] ATS 16 (signed and entered into force 31 October 1996); *Agreement between the Government of Australia and the Government of the French Republic regarding the Exchange and Reciprocal Protection of Classified Information* [2017] ATS 6 (signed and entered into force 7 December 2016).

109 [2002] ATS 25.

'The recipient Party shall afford the information a degree of protection equivalent to that afforded it by the releasing Party'.[110] The only two specific references to law are:

> Each Party shall protect classified information received directly or indirectly from the other Party according to the terms set forth herein and in accordance with its laws and regulations.[111]
>
> [and]
>
> All individuals having access to the information are informed of their responsibilities to protect the information in accordance with applicable laws and regulations.[112]

3.25 The Department of Foreign Affairs and Trade (DFAT) National Interest Analysis identified that:

> [The] underlying obligation placed on Australia and the United States is to protect each other's classified information in a similar manner to how it protects its own classified information of corresponding security classification.[113]

3.26 DFAT concluded the agreement could be implemented by existing policy:

> No changes to domestic laws or policy are required to implement the proposed Agreement. The proposed Agreement can be implemented through the Commonwealth Protective Security Manual,[114] which sets out the procedures covered by the Agreement.[115]

3.27 I agree with DFAT's conclusion. It appears that the United States has taken a similar view, as we have not identified any express reference to protecting Australian (or other partner) agreements in US law.

---

110 *Agreement between the Government of Australia and the Government of the United States of America on the Reciprocal Protection of Classified Information*, signed 25 June 2002, ATS 25 (entered into force 27 August 2002) art 4 ('*Australia and USA Agreement on Classified Information')*

111 *Australia and USA Agreement on Classified Information* (n 110) art 1.

112 *Australia and USA Agreement on Classified Information* (n 110) art 6(D).

113 Department of Foreign Affairs and Trade (DFAT), 'National Interest Analysis', *Agreement between the Government of Australia and the Government of the United States of America on the Reciprocal Protection of Classified Information* (Document, 27 August 2002) [12].

114 The Commonwealth Protective Security Manual was the precursor to the Australian Government Protective Security Policy Framework (PSPF). The Protective Security Manual was described as more compliance based than the principles-based approach taken by the PSPF. See Australian National Audit Office, *The Management of Physical Security* (Report No 49, 24 June 2014).

115 DFAT, 'National Interest Analysis', *Australia and USA Agreement on Classified Information* (Document, 27 August 2002) [14].

3.28 Another example is the agreement with France: the *Agreement between the Government of Australia and the Government of the French Republic regarding the Exchange and Reciprocal Protection of Classified Information*. That agreement provides:

> the Recipient Party shall provide Classified Information transferred or received from the Originating Party protection to a standard no less than that given to the Recipient Party's own national Classified Information of corresponding Security Classification as provided …[116]

3.29 The DFAT National Interest Analysis concludes:

> No amendment to Australian law is required to implement the proposed Agreement. The proposed Agreement is implemented by laws and policies in place relating to protective security. The Australian Government Protective Security Policy Framework (PSPF) requires agencies to adhere to the provisions of any international security of information agreements. The proposed Agreement will not require any change to the existing roles of the Australian Government or the State and Territory governments.[117]

3.30 DFAT analysis of other treaties for the mutual protection of classified information draws similar conclusions.[118]

3.31 The Protective Security Policy Framework (PSPF), which is discussed in **Chapter 4**, recognises Australia's obligations under international information sharing agreements. In particular, Policy 7: Security Governance for International Sharing under the PSPF (PSPF Policy 7) requires Australian Government entities to 'safeguard security classified foreign entity information or assets in accordance with the provisions set out in the agreement or arrangement'. This includes applying equivalent classification markings where these have been established.[119]

---

116 *Agreement between the Government of Australia and the Government of the French Republic regarding the Exchange and Reciprocal Protection of Classified Information* [2017] ATS 6 (signed and entered into force 7 December 2016) art 6.1(a).

117 DFAT, 'National Interest Analysis', *Agreement between the Government of Australia and the Government of the French Republic regarding the Exchange and Reciprocal Protection of Classified Information* [2017] ATNIA 5 (Document, 7 December 2016) [25].

118 For example: DFAT, 'National Interest Analysis', *Agreement between the Government of Canada and the Government of Australia Concerning the Protection of Defence Related Information Exchanged between Them* [1996] ATNIA 25; DFAT, 'National Interest Analysis', *Agreement Between the Government of Australia and the North Atlantic Treaty Organisation on the Security of Information* [2008] ATNIA 27 (Document, 26 November 2008) [23]; DFAT, 'National Interest Analysis', *Agreement between the Government of Australia and the Government of the Republic of Singapore for the Reciprocal Protection of Classified Information Transmitted Between the Australian Department of Defence and the Singapore Ministry of Defence* [1996] ATNIA 46 (Document, 29 October 1996).

119 Department of Home Affairs, *Protective Security Policy Framework, Policy 7: Security Governance for International Sharing* (Policy No 7, November 2021) 1-4. Agreements with this requirement that are mentioned in PSPF Policy 7 include those with the European Union, France, Japan and the United

3.32 Australia's international obligations under information sharing agreements can, and are, implemented through policy and do not require specific provisions to be enacted in Australian domestic law. Nevertheless, the *Criminal Code* should provide no less protection to information in the possession of Australian agencies that originated with a partner than it does to its own information (this requirement is incorporated in **Recommendations 2** and **6**).

Implied freedom of political communication

3.33 In addition to Australia's international obligations, it is imperative that constitutional limitations be observed in drafting Commonwealth laws. The main constitutional limitation that is relevant to Part 5.6 of the *Criminal Code* is the implied freedom of political communication. The implied freedom is not as broad as art 19 of the ICCPR. Many academics have said that the implied freedom alone is insufficient to adequately protect the important role of a free press in a liberal democracy. Unlike other Five Eyes countries that have some form of express constitutional or other protection for free speech, the minimal protection of the implied freedom of political communication is the only domestic guarantee relating to 'free speech' in Australia at a Commonwealth level.[120]

3.34 In 2004 the Australian Law Reform Commission report *Keeping Secrets: The Protection of Classified and Security Sensitive Information* recommended that the government review the constitutionality of secrecy provisions.[121] In a later report the ALRC noted that 'catch-all' offences may not 'sit comfortably with the implied constitutional freedom of communication'.[122]

3.35 The High Court has held that an implied freedom of political communication exists as an indispensable part of the system of representative and responsible government created by

States. Whether the automatic application of equivalent security classifications in this manner is consistent with s 90.1(1)(a) of the *Criminal Code* is discussed in Chapter 4.

120 See, eg, Rebecca Ananian-Welsh, Sarah Kendall and Richard Murray, 'Risk and Uncertainty in Public Interest Journalism: The Impact of Espionage Law on Press Freedom' (2021) 44(3) *Melbourne University Law Review* 769; Hannah Ryan, 'The Constitutional Cost of Combatting Espionage and Foreign Interference' (2018) 47(1) *Law Society of NSW Journal* 73, 75; Kylie Weston-Scheuber, 'Hear No Evil, See No Evil, Speak No Evil: The Secretisation of Information by Government in Australia' (2022) 34(1) *Bond Law Review* 31, 87; Rebecca Ananian-Welsh, '"*Smethurst v Commissioner of Police*" and the unlawful seizure of journalists' private information' (2020) 24(1) *Media and Arts Law Review* 69; Keiran Hardy and George Williams, 'Press Freedom in Australia's Constitutional System' (2021) 7(1) *Canadian Journal of Comparative and Contemporary Law* 244, 252–3.

121 Australian Law Reform Commission (ALRC), *Keeping Secrets: The Protection of Classified and Security Sensitive Information* (Report No 98, May 2004) 19, Recommendation 5-5.

122 ALRC, *Secrecy Laws and Open Government in Australia* (Report No 112, December 2009) 137 [4.151].

the Constitution.[123] It operates as a freedom from government restraint rather than a right conferred directly on individuals.[124] The test for whether a law infringes the implied freedom of political communication has been developed in a series of High Court decisions, most recently in *McCloy v New South Wales*[125] (*McCloy*) and *Brown v Tasmania*[126] (*Brown*).

3.36 The test of structured proportionality outlined in *McCloy* as modified in *Brown* is broadly as follows:

- Does the law effectively burden the implied freedom in its terms, operation or effect?
- If there is a burden, are the purpose of the law and the means adopted to achieve that purpose legitimate, in the sense that they are compatible with the maintenance of the constitutionally prescribed system of representative government?
- If there is a legitimate purpose, is the law reasonably appropriate and adapted to advance that legitimate object? (This question involves what is referred to as 'proportionality testing' to determine whether the restriction is suitable, necessary and adequate on the balance).[127]

3.37 The issue of whether secrecy offences affecting public servants infringe the implied freedom of political communication was the subject of judicial consideration in *Bennett v President, Human Rights and Equal Opportunity Commission*[128] (*Bennett*). In *Bennett*, Justice Finn held that then reg 7(13) of the *Public Service Regulations 1999*, which imposed a duty on officials to maintain the secrecy of *all* official information regardless of whether its disclosure might cause harm to the public interest, was invalid, as it was contrary to the implied freedom of political communication. Subsequently, in *R v Goreng-Goreng*,[129] Justice Refshauge held that reg 2.1 of the *Public Service Regulations 1999*, which replaced reg 7(13) and introduced a harm element prohibiting the disclosure of information if it was reasonably foreseeable that the disclosure could be prejudicial to the effective working of government, was not invalid, as it did not breach the implied freedom of political communication. Regulation 7(3) of the *Public Service Regulations 2023* now relevantly provides:

> An APS employee must not disclose information that the APS employee obtains or generates in connection with the APS employee's employment if it is reasonably foreseeable that the

123 *Nationwide News v Wills* (1992) 177 CLR 1; *Australian Capital Television Pty Ltd v Commonwealth* (1992) 177 CLR 106; *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520.
124 *Comcare v Banerji* (2019) 267 CLR 373, [20].
125 (2015) 257 CLR 178.
126 (2017) 261 CLR 328.
127 *McCloy v New South Wales* (2015) 257 CLR 178, 193–5; *Brown v Tasmania* (2017) 261 CLR 328, 362 [104].
128 (2003) 134 FCR 334.
129 (2008) 2 ACTLR 238.

> disclosure could be prejudicial to the effective working of government, including the formulation or implementation of policies or programs.

3.38 Regulation 7(4) also provides:

> An APS employee must not disclose information that the APS employee obtains or generates in connection with the APS employee's employment if the information:
>
> (a) was, or is to be, communicated in confidence within the government; or
>
> (b) was received in confidence by the government from a person or persons outside the government;
>
> whether or not the disclosure would found an action for breach of confidence.

3.39 *Comcare v Banerji*[130] (*Banerji)* is a more recent examination of the interaction between the implied freedom of political communication and the validity of laws that control the actions of public officials. However, this case did not involve a secrecy provision. Instead, it concerned the Australian Public Service (APS) Code of Conduct. In *Banerji*, the High Court held that the requirement in s 13(11) of the *Public Service Act 1999* (Cth) – that employees behave in a way that upholds APS values and the integrity and good reputation of the APS – did not infringe the implied freedom of political communication. Ms Banerji's employment with the Department of Immigration and Citizenship was terminated after she was identified as the author of various anonymous tweets criticising government policy. Ms Banerji sought compensation under the *Safety, Rehabilitation and Compensation Act 1988* (Cth) (*SRC Act*) for psychological injury arising out of the termination. Comcare rejected the claim on the basis that her termination was 'reasonable administrative action' for the purpose of the exception to the definition of 'injury' in s 5A(1) of the *SRC Act*. The Administrative Appeals Tribunal set aside this decision on the basis that the termination was unlawful because it infringed the implied freedom of communication. An appeal to the Federal Court was then removed into the High Court.

3.40 The High Court held that the relevant provisions of the *Public Service Act* were not invalid, as they did not impose an unjustified burden on the implied freedom of political communication, and the termination of Ms Banerji's employment was not unlawful. The Court accepted that the relevant provisions of the *Public Service Act* did burden political communication; however, the purpose of the provisions was held to be legitimate in that the maintenance of an apolitical and impartial APS was consistent with the system of government established by the Constitution.[131] The provisions were also held to be appropriate and adapted to achieving this legitimate purpose – in particular, noting that the operation of the

130 (2019) 267 CLR 373.

131 *Comcare v Banerji* (2019) 267 CLR 373, [30]–[31] (Kiefel CJ; Bell, Keane and Nettle JJ).

provisions and the range of penalties that could be imposed reflected a reasoned and focused response to the need to ensure that the requirements of upholding APS values trespassed no further upon the implied freedom than is reasonably justified.[132]

3.41 While the High Court's decision in *Banerji* did not concern the contravention of a secrecy offence, it suggests that under the implied freedom, government regulation of the disclosure of information by public officials may be permissible to a greater degree than it would be for members of the general public. Nevertheless, caution must be exercised, as the consequences and thus proportionality of an administrative sanction, including loss of employment, is considerably less than a criminal sanction, which may result in imprisonment.

3.42 At the time the EFI Bill was being considered in 2018, the Attorney-General's Department (AGD) advised the Parliamentary Joint Committee on Intelligence and Security (PJCIS) that it had considered the implied right to freedom of communication and 'is confident that the offences in the Bill do not infringe on the implied freedom'.[133]

3.43 Some submitters to the PJCIS inquiry into the EFI Bill took a different view. For example, the Law Council of Australia noted that some parts of the EFI Bill 'may be invalid on the basis that they infringe the constitutional protection of freedom of political communications'.[134] The Australian Lawyers Alliance, the Human Rights Law Centre (HRLC), AHRC and others made similar points.[135]

3.44 It its submission to the 2023 AGD *Review of Secrecy Provisions*, and its submission to this review, the Law Council of Australia again noted that 'it is likely that "catch-all" secrecy offences, that fail to distinguish between categories of information, categories of persons and fails to specify a harm requirement, will not meet the standard of justification' set out in *McCloy*.[136] Submissions to this review from the HRLC and academics took a similar view.[137] This is particularly relevant to the deemed harm offence (**Chapter 4**), the proposed new general offence (**Chapter 7**) and offences that apply to non-officials (**Chapter 8**).

---

132 See *Comcare v Banerji* (2019) 267 CLR 373, [32]–[42] (Kiefel CJ; Bell, Keane and Nettle JJ). Justices Gageler, Gordon and Edelman each delivered separate concurring judgments.

133 Attorney-General's Department (AGD), Supplementary Submission No 6.1 to PJCIS, *Inquiry into the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (13 February 2018) 74 ('*PJCIS EFI Bill Review*').

134 Law Council of Australia, Submission No 5 to *PJCIS EFI Bill Review* (n 133) (22 January 2018) 55–6.

135 Human Rights Law Centre (HRLC), Submission No 11 to *PJCIS EFI BILL Review* (n 133) (22 January 2018) 14; Australian Lawyers Alliance, Submission No 12 to *PJCIS EFI Bill Review* (n 133) (22 January 2018) 18; AHRC, Submission No 17 to *PJCIS EFI Bill Review* (n 133) (24 January 2018) 4–5; Dr Luke Beck, Submission No 41 to *PJCIS EFI Bill Review* (n 133) (2 March 2018) 1.

136 Law Council of Australia, Submission (ID No 44186415) to AGD, *Review of Secrecy Provisions* (22 May 2023) [41]; Law Council of Australia, *Submission 19*, 13.

137 HRLC, *Submission 14*, 2; Joint Academic Submission, *Submission 13*, 13.

Chapter 4: Offences with a 'deemed harm' element

4.1 This chapter deals with the deemed harm offence in s 122.1 of the *Criminal Code*. Section 122.1(1) makes it an offence punishable by a maximum of 7 or 10 years imprisonment for a Commonwealth officer or other person engaged to perform work for a Commonwealth entity to recklessly communicate 'inherently harmful information' obtained in connection with their work for the Commonwealth.[138] 'Inherently harmful information' is a defined term which covers any information that an official has classified as 'secret' or 'top secret' in accordance with a policy framework, as well as a wide range of information connected to intelligence agency functions and 'law enforcement'.

4.2 This chapter starts by explaining what is meant by 'deemed harm' and different views on when deemed harm offences are appropriate. It then discusses the 3 elements of the term 'inherently harmful information' in detail and makes findings and recommendations on each element.

4.3 The communication offence in s 122.1(1) has a related 'dealing with' offence in s 122.1(2). The 'dealing with' offences are discussed in **Chapter 6**, as are the other associated offences.

Deemed harm

4.4 Criminal offences have a physical and a fault (mental) element. In the context of the offence in s 122.1, 'deemed harm' means that, for the physical element of the offence, the prosecution does not have to prove that any actual harm occurred or was likely to occur as a result of communicating or 'dealing with' the information; only that the information falls within what has been defined as 'inherently harmful information'.[139]

---

138 The higher penalty of up to 10 years imprisonment applies in a range of aggravating circumstances – see Chapter 6. The meaning of 'Commonwealth officer' and 'engaged to perform work for a Commonwealth entity' is discussed in Chapter 1.

139 The other elements of the offence also need to be made out: the communication or dealing must be intentional; the person must be reckless as to whether the information is 'inherently harmful information'; and, they must be reckless as to the fact that they obtained the information by reason of being or having been a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity.

4.5 The general conclusion of previous reviews is that there should ordinarily be an express harm element in secrecy offences.[140] Scope for 'deemed harm' or harm automatically attributed to a class of information has been accepted only for a narrow set of *specific* offences where there would inevitably be harm to an *essential public interest* (as opposed to general secrecy offences of the type in the *Criminal Code*).[141]

4.6 The Australian Law Reform Commission (ALRC) 2009 report *Keeping Secrets: The Protection of Classified and Security Sensitive Information* (ALRC 2009 Secrecy Laws Report) stated that 'the role of the criminal law in publicly punishing, deterring, and denouncing offending behaviour is appropriate when applied to behaviour that harms, is reasonably likely to harm or intended to harm essential public interests'.[142] The ALRC accepted that in very limited circumstances an express harm requirement may not be the most effective way to address the harm caused by the disclosure of certain kinds of information, including intelligence information.[143] Recommendation 8-2 in the ALRC's report was that specific secrecy offences should include an express harm requirement except, relevantly, where the offence covers a narrowly defined category of information and the harm to an essential public interest is implicit.[144]

4.7 The Law Council of Australia's submission to this review strongly agreed with the principles and recommendations in the ALRC's report. One of the issues the Law Council and other submissions raised is that the deemed harm offence in s 122.1 of the *Criminal Code* is much wider than the ALRC's recommended approach to deemed harm offences. In particular, the Law Council submitted that key definitional concepts such as 'inherently harmful information' are unjustifiably broad and pick up a vast range of information with variable likelihood of causing harm.[145]

4.8 During consideration of the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 (EFI Bill), the Parliamentary Joint Committee on Intelligence and

---

140 See, eg, Australian Law Reform Commission (ALRC), *Keeping Secrets: The Protection of Classified and Security Sensitive Information* (Report No 98, May 2004) 18, recommendation 5-3 ('*ALRC 2004 Secrecy Laws Report*'); ALRC *Keeping Secrets: The Protection of Classified and Security Sensitive Information* (Report No 112, December 2009) 23–4, 307–8 ('*ALRC 2009 Secrecy Laws Report*'); Roger Gyles, INSLM (former), *Report on the Impact on Journalists of Section 35P of the ASIO Act* (Report, October 2015) ('*INSLM Report on Section 35P of the ASIO Act*'); Senate Environment and Communications References Committee, Parliament of Australia, *Freedom of the Press* (Report, May 2021) 35 [3.20]. Also see Annex B.

141 *ALRC 2009 Secrecy Laws Report* (n 140) 279 [8.24].

142 *ALRC 2009 Secrecy Laws Report* (n 140) 118 [4.77].

143 *ALRC 2009 Secrecy Laws Report* (n 140) 306-307 [8.143]-[8.144].

144 *ALRC 2009 Secrecy Laws Report* (n 140) 307.

145 Law Council of Australia, *Submission 19*, 11 [9].

Security (PJCIS) and the Attorney-General's Department (AGD) expressly acknowledged that the Part 5.6 offences are wider than the ALRC recommended.[146] AGD said that the s 122.1 offence departs from the ALRC's recommendations by being premised on certain categories of information being 'inherently harmful' rather than including an express harm requirement.[147]

4.9 Principle 4 of the AGD *Review of Secrecy Provisions* (AGD Review of Secrecy Provisions) says that a harm-based approach should be taken to framing secrecy offences and that, where deemed harm is used, it should 'cover a narrowly defined category of information where the harm to an essential public interest is implicit, or protect against harm to the relationship of trust between individuals and the Government integral to the regulatory functions of government'.[148] In its submission to this review, AGD submitted that retaining a deemed harm offence in s 122.1 was appropriate and consistent with Principle 4 of the AGD Review of Secrecy Provisions report.[149] AGD stated:

> [This aspect of Principle 4] recognises that for some types of information, the substantial risk of harm to an essential public interest is clear to a potential discloser from the type or classification of the information. This can include some types of national security and law enforcement information, including information obtained or generated by intelligence agencies, or information that has been assessed and marked as SECRET or TOP SECRET. In such circumstances, it can be appropriate for the elements of the offence to refer to the type or classification of the information instead of the consequences of its disclosure …[150]

4.10 At the time the EFI Bill was being debated, AGD said the definition of 'inherently harmful information' was 'exhaustive' and the categories of information covered 'necessarily narrow'.[151] For the reasons discussed later in this chapter, I do not agree with this characterisation.

4.11 The Department of Home Affairs stated that in recent years it has generally pursued the introduction of specific secrecy offences with a deemed harm element.[152] The Department's

---

146 Parliamentary Joint Committee on Intelligence and Security (PJCIS), Parliament of Australia, *Advisory Report on the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (Report, June 2018) 103 [4.21] ('*PJCIS EFI Bill Report*').

147 Attorney-General's Department (AGD), Submission No 6 to PJCIS, *Inquiry into the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (January 2018) 31 [102] ('*AGD Submission to PJCIS Inquiry into EFI Bill*').

148 *ALRC 2009 Secrecy Laws Report* (n 140) 307-8.

149 AGD, *Submission 7*, 8 [28]; AGD, *Review of Secrecy Provisions* (Final Report, 21 November 2023) 21 [62] ('*AGD Review of Secrecy Provisions*').

150 AGD, *Submission 7*, 8 [30].

151 *AGD Submission to PJCIS Inquiry into EFI Bill* (n 147) 31 [102].

152 Department of Home Affairs (Home Affairs), *Submission 2*, 4.

submission suggested that the use of a deemed harm offence and the concept of 'inherently harmful information' provided the following benefits:

> Clarity – specific offences tied to types of information provide certainty as to what type of information is captured by a given offence. …
>
> Deterrence – in combination with the clarity provided by deemed harm offences, such offences have a clear, but targeted, deterrent effect, particularly in instances where the specific offences carry a higher penalty. …
>
> Tailoring – deemed harm offences allowing for the tailoring of the application of the offence and any defences to the particular issue. …[153]

4.12 The Department of Home Affairs also stated that, in its view, the incorporation of an actual harm element into a secrecy offence of general application to intelligence information can present unintended difficulties in prosecutions and makes them more complex. Further, the Department of Home Affairs said that, in the context of national security information, meeting the requirements of proving harm could 'potentially present insurmountable challenges for the prosecution'.[154] For the reasons discussed in this chapter, I find that the deemed harm offence in s 122.1 is neither clear in its application nor well-tailored. It also contains what must be assumed to be unintended difficulties that may make a prosecution difficult, particularly in relation to classified information.

4.13 Most of the intelligence agencies favoured retaining the deemed harm offences in their own Acts in addition to the existing deemed harm offence in s 122.1 of the *Criminal Code*.[155]

4.14 I agree that there is a place for a deemed harm offence relating to some national security and law enforcement related information in Part 5.6 of the *Criminal Code*. However, any such deemed harm offence should be limited to narrowly defined categories of information, where there is a sufficiently high likelihood that harm to a critical national interest will always or almost always result from disclosure. The categories of information covered by a deemed harm offence must also be clearly defined by the parliament. For the reasons discussed in

153 Home Affairs, *Submission 2*, 5.

154 Home Affairs, *Submission 2*, 6.

155 Home Affairs, *Submission 2*, 4–7; Australian Signals Directorate (ASD), *Submission 4*, 6 [18]; Defence Intelligence Group (DIG), *Submission 5*, 1–6; Australian Secret Intelligence Service (ASIS), *Submission 10*, 6–9; Office of National Intelligence (ONI), *Submission 8*, 10–11; AUSTRAC, *Submission 15*, 6–7; Australian Criminal Intelligence Commission (ACIC), *Submission 16*, 2; Australian Security Intelligence Organisation (ASIO), *Submission 6*, 5–6: However, ASIO also recognised that there may be other ways of meeting their objectives.

the rest of this chapter, the current definition of 'inherently harmful information' does not meet these tests.

4.15 The Issues Paper for this review identified that in other Five Eyes countries deemed harm offences generally only apply to members of security and intelligence services, as opposed all Commonwealth officers and others who perform work for a Commonwealth entity.[156] Whether this approach should be followed in Australia was considered during the course of this review. Security and intelligence agencies highlighted that in Australia there are many officials who work outside of intelligence and security agencies who have access to significant amounts of highly sensitive information (e.g. some Australian Defence Force members). There are also many individuals who receive copies of highly sensitive intelligence reports or receive intelligence briefings in the course of their duties, including officials in Departments such as the Department of Home Affairs, the Department of Prime Minister and Cabinet, AGD and the Department of Foreign Affairs and Trade. The argument put forward by the intelligence agencies is essentially that officials who are entrusted with the same types of official information should be subject to the same offences.

4.16 I agree that it is reasonable for appropriately narrow deemed harm offences (of the type recommended in this Chapter) to apply to all Commonwealth officers and others who perform work for a Commonwealth entity. Where officials, including intelligence officials, hold a particular position of trust, recognised by the granting of the highest level of security clearance, there is additional culpability for breach of that trust. This can be appropriately recognised by an increased penalty (as discussed in **Chapter 6**) rather than by a separate offence. Accepting that all officials should be subject to the offence in s 122.1 reduces or removes the need for there to be separate offences specific to intelligence officials.

Inherently harmful information

4.17 'Inherently harmful information' is defined in s 121.1(1) and has 3 parts:

> ***inherently harmful information*** means information that is any of the following:
>
> (a) security classified information;
>
> (c) information that was obtained by, or made by or on behalf of, a domestic intelligence agency or a foreign intelligence agency in connection with the agency's functions;
>
> (e) information relating to the operations, capabilities or technologies of, or methods or sources used by, a domestic or foreign law enforcement agency.[157]

156 INSLM, *Review of Secrecy Offences in Part 5.6 of the Criminal Code 1995: Issues Paper* (January 2024) 31–32 [2.14]–[2.17] ('*INSLM Issues Paper*').

157 *Criminal Code Act 1995* (Cth) s 122.1 ('*Criminal Code*').

4.18 Each part of this definition contains terms that are further defined. One term that applies to them all is 'information' (which has the meaning given by s 90.1):

> ***information*** means information of any kind, whether true or false and whether in a material form or not, and includes:
>
> (a) an opinion; and
>
> (b) a report of a conversation.[158]

4.19 As the Law Council of Australia notes, courts have interpreted the term 'information' broadly – for example, to extend to not only the acquisition of an opinion but the drawing of an inference that ought reasonably to have been formed based on known facts; and factual knowledge either of a concrete kind or obtained by means of suggestion from which knowledge can be imputed.[159] The breadth of the definition of 'information', combined with the over-broadness of the categories that make up the definition of 'inherently harmful information', mean that the deemed harm offence captures a very wide range of conduct with a significant variation in likelihood of harm.

Security classified information

4.20 The first part of the definition of 'inherently harmful information' in s 121.1(1) is 'security classified information'. 'Security classified information' means 'information which has a security classification'. 'Security classification' has the meaning given by s 90.5(1):

> (1) ***Security classification*** means:
>
> (a) a classification of secret or top secret that is applied in accordance with the policy framework developed by the Commonwealth for the purpose (or for purposes that include the purpose) of identifying information:
>
> (i) for a classification of secret – that, if disclosed in an unauthorised manner, could be expected to cause serious damage to the national interest, organisations or individuals; or
>
> (ii) for a classification of top secret – that, if disclosed in an unauthorised manner, could be expected to cause exceptionally grave damage to the national interest; or
>
> (b) any equivalent classification or marking prescribed by the regulations.
>
> (1A) For the purposes of a reference, in an element of an offence in this Part, to security classification, strict liability applies to the element that:
>
> (a) a classification is applied in accordance with the policy framework developed by the Commonwealth for the purpose (or for purposes that include the

158 *Criminal Code* (n 157) s 90.1

159 Law Council of Australia, *Submission 19*, 18–19 [39]–[41], referring to *Crowley v Worley Limited* [2022] FCAFC 33 [4]–[5], [164]–[178]; *Regina v Rivkin* [2004] NSWCCA 7 [127] citing *Hooker Investments Pty Limited v Baring Bros Halkerston and Partners Securities Limited* (1986) 10 ACLR 462, 468.

purpose) of identifying the information mentioned in subparagraph (1)(a)(i) or (ii); or

(b) a classification or marking is prescribed by the regulations as mentioned in paragraph (1)(b).

…

No regulations have been made for the purpose of s 90.5(1)(b).

4.21 Strict liability applies to the element of the offence that a 'classification is applied in accordance with the policy framework' (s 90.5(1)(a)), which means that there is no fault (mental) element and the defence of mistake of fact applies (see ss 6.1 and 9.2 of the *Criminal Code*). Strict liability and the fault (mental) element for security classified information are discussed later in this chapter.

4.22 The offences for non-Commonwealth officials in s 122.4A, discussed further in **Chapter 8**, also applies if 'information has a security classification of secret or top secret'. That wording is slightly different from the terminology of 'security classified information' used in s 122.1. To the extent that the definition of 'security classification' is picked up, it would not apply to any additional equivalent classification prescribed by the regulations.

4.23 Government agencies have been operating on the basis that the 'policy framework' referred to in the definition of 'security classified information' in s 90.5 is the Protective Security Policy Framework (PSPF).

4.24 On the government's protective security website the PSPF is described as being intended to 'help Australian Government entities to protect their people, information and assets, both at home and overseas'.[160] It sets out broad government protective security policy and 'supports entities to effectively implement the policy across 4 outcomes: security governance, information security, personnel security and physical security'. Under these outcomes are 16 policies. The most relevant to security classification decisions is Policy 8: Classifications System (PSPF Policy 8), which deals with how agencies are to 'correctly assess the security classification of their information and adopt marking, handling, storage and disposal arrangements that guard against information compromise'.[161] Policy 7: Security Governance for International Sharing (PSPF Policy 7) is about international information sharing arrangements. PSPF Policy 7 also contains requirements for how information is to be security classified. For example, agencies are required to mark foreign information as having the corresponding Australian security classification where relevant international agreements are

160 Home Affairs, 'Protective Security Policy Framework', Protective Security Policy Framework (Web Page, May 2024) <https://www.protectivesecurity.gov.au/about>.

161 Home Affairs, Protective Security Policy Framework, Policy 8: Classifications System (Policy No 8, August 2023) 1 ('*PSPF Policy 8*').

in place.[162] Policy 2: Management structures and responsibilities (PSPF Policy 2) includes requirements relating to security awareness training for officials and contractors.[163]

4.25 The primary arguments in favour of using security classification as an element of the offence are that it is a system familiar to Commonwealth officers and it provides a level of certainty as to what information the offence applies to. The primary arguments against using security classification as an element of an offence are that it introduces significant uncertainty and is inconsistent with the rule of law. Other points relevant to the use of security classification as an element of an offence include compliance with international obligations and its role in proof of 'recklessness'. Each of these is discussed below.

Does 'security classification' provide certainty?

4.26 As noted in the Office of National Intelligence (ONI) submission, persons who enter into a relationship with intelligence and security agencies, as an employee or contractor or through some other agreement or arrangement, gain privileged access to highly sensitive information.[164] On one view, it is reasonable to impose criminal sanctions on those individuals who may be characterised as 'trusted insiders' to ensure that classified information is handled in accordance with the policies that these officials are expected to adhere to.

4.27 At a surface level it appears there is a degree of certainty provided by relying on security classification as an element of a secrecy offence. In support of this view AGD stated:

> The department considers the definition of 'security classification' in section 90.5 of the Criminal Code is sufficiently clear for a criminal offence. The Protective Security Policy Framework Policy 8 (the PSPF Policy 8) provides clear requirements about classifying documents SECRET or TOP SECRET, including examples and guidance on when it is appropriate to classify documents as SECRET or TOP SECRET.[165]

4.28 In oral evidence at the public hearing, AGD also noted that s 90.5(1)(a)(i)–(ii) picks up the language of the PSPF relating to the classifications of 'secret' and 'top secret'.[166]

4.29 On the surface, an offence based on the disclosure of information that is classified as secret or top secret seems like a reasonable approach. Officials with training and security clearances who deal with security classified information on a regular basis can be expected to understand what these markings mean. Noncompliance with the security classification

---

162 Home Affairs, Protective Security Policy Framework, Policy 7: Security Governance for International Sharing (Policy No 7, November 2021) 4 [20]–[21] ('*PSPF Policy 7*').

163 Home Affairs, Protective Security Policy Framework, Policy 2: Management Structures and Responsibilities (Policy No 2, August 2023).

164 ONI, *Submission 8*, 7[62]–[64].

165 AGD, *Submission 7*, 11 [49].

166 Ms Sarah Chidgey, AGD, *Public hearing transcript*, 26 March 2024, 147.

requirements can and does result in administrative and disciplinary sanctions, including potential loss of employment (**Chapter 1**). There is a certain logic to applying criminal penalties for the same behaviour in cases where administrative and disciplinary sanctions are insufficient.

4.30 However, when this issue is examined in detail, it is apparent that there are many uncertainties in establishing what information is 'security classified information' within the meaning of the *Criminal Code*. These include, the following, as well as a range of technical issues:

- whether the information has to be *properly* classified
- what happens in the case of inconsistency between the PSPF and the requirements of s 90.5(1)(a)
- whether the PSPF and associated training and guidance support sufficiently accurate decision-making for criminal law purposes
- what evidence would need to be provided to establish a classification was 'in accordance with' the policy framework.

Each of these is discussed below. A more fundamental issue is whether incorporating a policy into the criminal law in this way is consistent with the rule of law. This is also discussed below.

Classified or properly *classified?*

4.31 The definition of 'security classified information' requires that a classification of secret or top secret be 'applied in accordance with the policy framework'. This raises a threshold question of whether, in order to establish the physical element of this part of the offence, the prosecution has to prove beyond reasonable doubt that information was properly or correctly classified under the PSPF or only the fact that a classification was applied.

4.32 As I said in my opening remarks on day 1 of the public hearing, a number of submissions suggested there was a difference of opinion on this issue.[167] Some suggested that the Crown has to prove that every classification was applied properly in accordance with the PSPF. Others seem to suggested that all that is required is that the document has a marking of 'secret' or 'top secret' on it.

4.33 The competing arguments were described in the Issues Paper:

> Counsel for a defendant would likely argue that this requires the Crown to lead evidence to prove that, if disclosed in an unauthorised manner, the information could be expected to cause serious damage to the national interest, organisation or individuals (in the case of SECRET) or exceptionally grave damage to the national interest (in the case of TOP SECRET). This would potentially be the same evidence that would be required if these harm elements

167 Mr Jake Blight, INSLM, *Public hearing transcript,* 25 March 2024, 6.

> were expressly incorporated in the offence. The Crown might seek to argue that it was sufficient for the prosecution to establish that at some stage some official had classified the information as SECRET or TOP SECRET in accordance with that official's understanding of the policy. This in turn might open an argument about the making of that assessment and whether it was in fact 'in accordance with' the policy.[168]

4.34 The Law Council of Australia was among the submitters raising concerns about the definition of 'security classified information'. It agreed with the Issues Paper that the use of the phrase 'in accordance with the policy framework' in s 90.5 is likely to lead to disputes about whether particular information was properly classified according to the PSPF.[169] The joint academic submission noted that it was not clear whether the phrase 'in accordance with the policy framework' in s 90.5 means simply that information was classified under the framework or that it was classified properly. The joint academic submission suggested that a way to avoid a possible constitutional problem was to interpret the provision so that it *does* require proof of correct classification because this approach ensures Ch III courts have the capacity to independently assess every element of a criminal offence.[170]

4.35 Even among government agencies, there was a degree of inconsistency and uncertainty in submissions on what is required to establish that information is classified 'in accordance with' the PSPF. In the AGD Review of Secrecy Provisions, the Department said that the definition of 'security classified information' requires 'the prosecution … to prove that the security classification is applied in accordance with the policy framework developed by the Commonwealth for the purposes of information protection (currently the Protective Security Policy Framework)'.[171] The Commonwealth Director of Public Prosecutions (CDPP) submission referred to the fact that s 90.5 required that a security classification be applied in accordance with the PSPF. It also noted that strict liability applies to this element of the offence and concluded that 'the prosecution only has to prove that the information has a security classification, and the accused was reckless as to that fact'.[172] In later correspondence the CDPP said:

> To prove that the information has a security classification, we anticipate the prosecution leading that evidence from a senior officer of the relevant agency (the originator of the information) …
>
> [PSPF Policy 8] sets out several requirements that each entity, as the originator of the information, must comply with which ultimately results in information being given a security classification …

---

168 *INSLM Issues Paper* (n 156) 37 [2.32].
169 Law Council of Australia, *Submission 19*, 19 [44].
170 Joint Academic Submission, *Submission 13*, 8–9.
171 *AGD Review of Secrecy Provisions* (n 149) 39 [169].
172 Commonwealth Director of Public Prosecutions (CDPP), *Submission 20*, 2–3.

> If the only way information can be given a security classification is by applying the policy framework and for some reason the policy framework was not applied, then the information would not be "security classified information". For example, let's assume an officer in a government department simply stamps a document "Top Secret" without any regard to the policy framework. In those circumstances the document would not meet the definition of "security classified information".
>
> … The strict liability in relation to that element applies only to the accused's state of mind. That is, the prosecution does not have to prove the accused's intention, knowledge, recklessness or negligence in relation to whether the policy framework was applied. The prosecution still has to prove the fact that the information was classified in accordance with the policy framework.[173]

4.36 This issue was raised with AGD at the public hearing. AGD said that in their view the prosecution would have to show that the information was *properly* classified:

> **MR JAKE BLIGHT:** … I just want to understand the, the policy intention of 90.5 … It says classified in accordance with the PSPF or the relevant policy framework. Is it your policy intention that the prosecution should have to show as a physical element, that the document or information was properly classified?
>
> **MS SARAH CHIDGEY:** Yes. So the definition of security classification means the prosecution would need to show, as that section outlines, that the SECRET or TOP SECRET classification was applied in accordance with the policy, but then it goes specifically to talk about the key elements, which are the relevant harms related to SECRET or TOP SECRET classifications.
>
> There's then a sort of nuance in how the offence works with fault elements as well. …
>
> So it requires recklessness as to the fact that information bears such a classification, but then strict liability at that further level as to whether it's been applied in accordance with the framework. But the prosecution would have to show that it was indeed SECRET or TOP SECRET information.
>
> …
>
> **MR BLIGHT:** So we don't have to show that the defendant knew that the classification was properly applied.
>
> **MS CHIDGEY:** Yes. …
>
> **MR BLIGHT:** But for the physical element of that component, the prosecution would still have to show that the document actually, objectively, had been properly classified.

---

173 Email from CDPP to INSLM, 27 March 2024.

> **MS CHIDGEY:** That's correct.
>
> **MR BLIGHT:** Thank you. That's an important clarification. And that proper classification would be guided by both the Protective Security Policy Framework and the bit of 90.5 that talks about, for example, for a classification of TOP SECRET that, if disclosed in an unauthorised manner, could be expected to cause exceptionally grave damage.
>
> **MS CHIDGEY:** That's correct.[174]

4.37 The above evidence suggests that the policy intention behind the operation of s 90.5 of the *Criminal Code* is that the prosecution would have to prove beyond reasonable doubt, as a physical element of the deemed harm offence in s 122.1 relating to security classified information, that information was *properly* classified in accordance with the PSPF. This would seem to require proof that disclosure of the information could be expected to cause serious or exceptionally grave damage of the type described in s 90.5(1), a *higher* degree of harm than the 'harm or likely harm' that has to be established for the offence in s 122.2.

4.38 Representatives of the Law Council of Australia expressed uncertainty about how proof of correct classification, if required, would work in a trial:

> I have very deep conceptual difficulty working out exactly how that would play out in a courtroom. It's clear that there are some parameters, and we know that there are definitions for the extent of harm under the PSPF guidelines or frameworks for TOP SECRET and SECRET. But exactly 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. I just don't know how it would be done. It's very difficult to work out how a defence lawyer or an accused person would be able to dig below the surface of all of that. I'm not 100% sure either that the Attorney-General's Department is correct in the way that they suggest that this issue is justiciable, either.[175]

4.39 Therefore, despite its apparent simplicity, there remains a great deal of uncertainty surrounding the operation of the definition of 'security classified information' in s 90.5 of the *Criminal Code*. I agree with AGD's view that the physical element of the offence of disclosing classified information requires proof that the information has been properly classified in accordance with a framework consistent with s 90.5(1)(a). I acknowledge the Law Council's point that it is unclear how this would operate in practice in terms of the appropriateness of a security classification being applied under a policy being tested in a court room.

---

174 *Public hearing transcript,* 26 March 2024, 147–148.

175 Mr Philip Boulten SC, Member, Law Council's National Criminal Law Committee, Law Council of Australia, *Public hearing transcript*, 26 March 2024, 163–164.

Inconsistency with section 90.5

4.40 Further uncertainty arises because of the interaction between s 90.5(1)(a) and PSPF Policy 8 and its associated policies.

4.41 As noted above, s 90.5(1)(a) describes the 'policy framework' as one which has the purpose (or purposes which include the purpose) of identifying information as secret (if disclosed in an unauthorised manner, could be expected to cause serious damage to the national interest, organisations or individuals) or top secret (if disclosed in an unauthorised manner, could be expected to cause exceptionally grave damage to the national interest). To the extent that a policy framework is inconsistent with these requirements it will not be a policy framework of the type described in s 90.5(1)(a). That means that a classification decision made under it may not result in a document having a 'security classification' for the purpose of the *Criminal Code*, either because the document itself does not have a classification consistent with the definition in s 90.5(1) or because, to the extent that the policy framework provides for a definition of secret or top secret that is inconsistent with the definition in s 90.5(1), that policy framework cannot be considered to be the relevant policy framework for the purposes of s 90.5(1).

4.42 PSPF Policy 8 relevantly contains a table that summarises which security classification is to be applied based on the expected harm that 'compromise of information confidentiality would be expected to cause':

			Security classified information			
	UNOFFICIAL	**OFFICIAL**	**OFFICIAL: Sensitive**	**PROTECTED**	**SECRET**	**TOP SECRET**
	No business impact	1 Low business impact	2 Low to medium business impact	3 High business impact	4 Extreme business impact	5 Catastrophic business impact
Compromise of information confidentiality would be expected to cause ➔	**No damage**. This information does not form part of official duty.	**No or insignificant damage.** This is the majority of routine information.	**Limited damage** to an individual, organisation or government generally if compromised.	**Damage** to the national interest, organisations or individuals.	**Serious damage** to the national interest, organisations or individuals.	**Exceptionally grave damage** to the national interest, organisations or individuals.

PSPF Policy 8 – Supporting requirements[176]

4.43 This table is broadly consistent with s 90.5(1)(a) apart from some minor differences in the types of damage to be considered (top secret in s 90.5(1)(a)(ii) can only consider the national interest whereas the PSPF refers to the national interest, organisations and individuals). The

176 *PSPF Policy 8* (n 161) 2.

categories are very broad and there is no definition of 'serious damage', 'exceptionally grave damage' or 'national interest'. However, this table is not the entirety of the policy framework that officials are obliged to consider. PSPF Policy 8 requires officials to follow other specified policies. These might arguably be taken to form part of the 'policy framework' referred to in the definition of 'security classified information' in s 90.5. Alternatively, they may be relevant to an assessment of whether a security classification has been applied in accordance with the PSPF itself. In particular, PSPF Policy 8 expressly refers to officials being required to comply with the *Sensitive Material Security Management Protocol* and the *Australian Government Security Caveat Guidelines* (Caveat Guidelines). Neither of these documents is publicly available.[177] As discussed later in this chapter, the Caveat Guidelines and the classified annex to those Guidelines, appear to require applying 'secret' or 'top secret' classifications in circumstances broader than those described in s 90.5(1)(a) and do not always require a specific assessment of whether 'serious' or 'exceptionally grave' damage of the relevant types can be expected to result from disclosure. In a sense they 'deem' the harm likely and require application of a secret or top secret classification. Therefore, an official may have correctly applied a marking of secret or top secret based on the Caveat Guidelines but there will be a question as to whether the information is 'security classified information' for the purpose of the relevant offences. A similar issue arises in relation to the policy of automatically adopting classification markings applied by officials in other countries under their policies.

4.44 Information that a foreign official has classified as secret or top secret under their own country's policies would quite possibly not be 'security classified information' under s 90.5, as the classification was not applied under the Australian policy framework. However, as noted above, PSPF Policy 7 does require Australian officials to automatically apply the classification of 'secret' or 'top secret' to any information provided by certain partners. For example, information marked as secret or top secret by the United States must be given the equivalent marking in Australia.[178] As a result, the policy does not oblige (or enable) Australian officials to consider if the information received from the United States would cause the type of serious damage or exceptionally grave damage to *Australia's* national interest described in s 90.5(1). In some situations, the information may cause serious or exceptionally grave damage to Australia's national interest, but that will not necessarily always be the case even if its disclosure causes some harm to international relations.[179] This means that

177 *PSPF Policy 8* (n 161) 11 [47].

178 *PSPF Policy 7* (n 162) 4 [20]–[21]. Equivalent markings are also set out in PSPF Policy 7 for information received from France, the European Union and Japan.

179 Guidance in PSPF Policy 8 indicates that a classification of top secret based on damage to international relations will be appropriate if the damage caused by the disclosure is 'directly provoking international conflict or causing exceptionally grave damage to relations with friendly countries', while a classification of 'protected' (lower than secret) is indicated if the damage is 'short-term damage or disruption to diplomatic relations': see *PSPF Policy 8* (n 161) 8.

information provided by partners or derived from partner information that is automatically marked as secret or top secret may not necessarily always be 'security classified information' within the meaning of s 90.5. That the harm-based offence in s 122.2 expressly deals with information that a foreign government has provided in confidence supports an interpretation of the definition of 'security classification' in s 90.5 as being connected to decisions made under the Australian policy framework and in respect of Australia's national interest and so on. This result is not necessarily consistent with the classified information sharing agreements mentioned in **Chapter 3**.

4.45 A further source of possible inconsistency between markings on documents and the definition in s 90.5 is where an electronic system has applied a marking in an automated or semi-automated manner. Some IT systems prompt users to amend the classification of emails at certain points (such as when an attachment is added or removed), and users have the ability to manually change a security classification on an email. However, a number of agencies gave evidence to the effect that some of their email systems automatically apply the same marking to a 'reply' email as to the original email, with the user only having the option of *increasing* the classification.[180] In this type of scenario, where the original email was properly classified as secret based on an attachment and the reply did not include the attachment, the reply would have to be classified as secret or top secret, even if the entirety of the message was 'here is the report you asked for' and 'thanks' with no attachment.[181] This leads to a larger question as to whether classification decisions are made with the accuracy required for an element of a criminal offence.

Accuracy of classification decisions

4.46 The process for classifying documents set out in the PSPF is primarily designed as a protective security measure: it provides officials with high-level guidance on how to classify information; what classification markings should look like; and how to handle documents that have been classified, including how they should be stored and who they can be shared with. The question for this inquiry is not whether the PSPF is appropriate and working well for that purpose. Rather, the question is whether it is appropriate for decisions made under the PSPF

180 ASD, *Supplementary response 26*, 3; ONI, *Supplementary response 28*, 1–2; DIG, *Classified supplementary response*, 2.

181 A survey conducted by the Inspector-General of Intelligence and Security (IGIS) as part of the *Preliminary Inquiry into the Application of National Security Classifications in ASIO, ASIS, ONI, ASD, AGO and DIO* (IGIS Security Classifications Inquiry) identified that intelligence agency staff considered emails to be most at risk of over-classification. See IGIS, *Preliminary Inquiry into the Application of National Security Classifications in ASIO, ASIS, ONI, ASD, AGO and DIO: Preliminary Inquiry Report* (Report, 25 February 2021) ('*IGIS Security Classifications Report*').

to form the basis of an offence under the criminal law. To explore this, the inquiry took evidence on how classification decisions are made in practice, including:

- whether guidance outside the PSPF is relied on
- how many officials can make decisions
- what training they receive
- whether there are any record keeping or auditing standards.

4.47 This evidence received is discussed in more detail in **Annex D**. In summary:

- Every official with a secret or top secret clearance is a classification decision-maker in relation to those classifications (this is many thousands of individuals).
- There is no clear system for recording when and why security classification decisions are made or in many cases who made them.
- There is no established process for review of security classification decisions. Also, there is no regular process of auditing security classification decisions, and no single body has oversight or responsibility for security classification decision-making within the whole National Intelligence Community (NIC).
- A high percentage of staff in NIC agencies complete an annual on-line 'security awareness' module, but that training only touches briefly on classification decision-making, among other topics.
- Where there is more specialised training on classification decision-making, that training is not compulsory and the uptake on that training is quite low. Some agencies do not keep records of how many staff have taken the training or when it was taken.
- Some training material emphasises that under-classification constitutes a security breach, while over-classification reduces the utility of intelligence products for customers and can lead to unnecessary costs in managing information.
- Examples of internal guidance materials provided variable levels of details. Some did little or no more than replicate the general guidance given in PSPF Policy 8. Some provided examples so broad that they would likely lead to decisions inconsistent with s 90.5(1)(a).
- There was no evidence that any of the training was targeted at helping officials understand that the classification decisions they make have consequences for the criminal law and what standard the criminal law requires to establish that a classification is 'in accordance with' the relevant policy framework and the requirements in Part 5.6.

4.48 It is important to note that this review was only of a sample of NIC agencies and their training materials and guidance. A more comprehensive audit of security classification training and

decision-making across the Commonwealth may be beneficial but is outside the scope of an INSLM review. Nevertheless, the sample was sufficient to identify real concerns about whether training and guidance on making classification decisions under the PSPF is sufficient to produce decision-making with the level of accuracy and consistency that is appropriate for decisions with such serious implications for the criminal law.

4.49 It is worth noting again that the guidance given in PSPF Policy 8 about classification categories is high-level. Concepts like 'serious harm to the national interest' and 'exceptionally grave damage to the national interest' are very uncertain, particularly as 'national interest' is not defined. PSPF Policy 8 does provide some examples of the 'business impact' that should guide classification decisions.[182] Some of these are fairly clear, at least in parts, if somewhat circular: the example given for exceptionally grave damage to international relations is 'directly provoking international conflict or causing exceptionally grave damage to relations with friendly countries'. Others give little real guidance: the example for the category of exceptionally grave damage to crime prevention, defence or intelligence operations is 'significantly affecting the operational effectiveness, security or intelligence operations of Australian or allied forces'.[183] Uncertainty in classification categories leaves a lot of room for doubt as to whether decisions made under the policy framework will have the level of consistency and accuracy that should be expected for decisions that have such a significant role in the criminal law as well as whether they will be consistent with s90.5(1)(a).

4.50 Some agencies explicitly recognise that there is a high degree of subjectivity in assessing the level of 'business impact'. For example, the internal ASD Classification Guide states that:

> Determining the business impact level can be subjective, it relies on the originator's own experience and skill. In determining the business impact level, the originator should refer to similar examples, the ASD Security Classification Tables…, or seek section, branch head or ASD Security assistance.[184]

4.51 The examples referred to in the 'Classification Tables' mentioned in this quote are largely military examples. Most are very general and even where intelligence is referred to it provides very broad categories. For example, top secret includes 'the methods used or success obtained by national intelligence services' and 'higher ASD and Department of Defence policy and strategy of an allied or inter-Service nature'. Examples for secret include 'briefing papers on highly sensitive Defence subjects for Australian delegates to top level

---

182 *PSPF Policy 8* (n 161) 7–8. Note that the policy allows agencies to develop their own 'sub-impact categories'. It is not clear if this agency-level guidance forms part of the 'policy framework', though it seems likely that many officials would make decisions primarily based on agency-level guidance. The PSPF does not provide agencies with any guidance on the requirements of s 90.5.

183 *PSPF Policy 8* (n 161) 8.

184 ASD, *Classified supplementary response*, Attachment D, 17 [6.13].

international conferences'. Reliance on this sort of broad guidance may well result in decisions inconsistent with 90.5(1)(a).

4.52 A number of agencies referred to the Inspector-General of Intelligence and Security (IGIS) Preliminary Inquiry into the Application of National Security Classifications in ASIO, ASIS, ONI, ASD, AGO and DIO (IGIS Security Classifications Preliminary Inquiry) as evidence that there was no problem with the way information is classified. For example, in its written submission ONI said:

> The IGIS found there was no evidence of systemic misunderstanding of the scope or application of classifications in the PSPF, which may have been expected if the PSPF was ambiguous or if thresholds for classifications (regardless of references to s90.5 of the Criminal Code) were too imprecise to allow consistent and defensible classification decisions.[185]

4.53 IGIS did not consider the interaction between the PSPF and the *Criminal Code.*

4.54 For the reasons outlined at **Annex E**, the purpose and findings of the IGIS Security Classifications Preliminary Inquiry do not support an argument that it is appropriate to use the PSPF and decisions made under it as the basis of serious criminal offence. While it is true that the IGIS Preliminary Security Classifications Inquiry did not find 'systemic' over-classification, it does not follow that each of the many thousands of documents that are classified each year are classified correctly. The IGIS Security Classifications Preliminary Inquiry also found that a significant percentage of agency staff did not consider their training or guidance on classification decisions was adequate.

4.55 It is also worth noting that a previous IGIS, the Hon. Margaret Stone, said in her comments on the EFI Bill that there was a tendency to over-classify documents 'to be safe'.[186] The New Zealand IGIS reached a similar conclusion.[187] The United States has a very complex system of presidential orders and laws about classification, classification review and restrictions on who

---

185 ONI, *Submission 8*, 9.

186 IGIS, Submission No 13 to PJCIS, *Inquiry into the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (January 2018) 7.

187 Office of the Inspector-General of Intelligence and Security (NZ), *A review of the New Zealand Classification System* (Report, August 2018). In this comprehensive review the NZ IGIS noted that 'classification systems have an inherent bias towards over-classification. This bias has been exhaustively analysed – particularly in the US – and is widely recognised…The essential problem is that security bureaucracies give officials powerful reasons to over-classify and little or no reason to avoid or challenge over-classification. There are rarely if ever any adverse consequences for an official who is seen as 'too careful'. Being – or being seen as – not careful enough can however mean professional disaster. Nor are there rewards, or generally much satisfaction, in challenging the classification decisions of others.' [106]

can make classification decisions,[188] as well as an entire office – the Information Security Oversight Office – dedicated to evaluating and improving classifications, particularly over-classification.

Evidence of classification decisions

4.56 To establish that a classification decision has been made in accordance with s 90.5(1)(a) and the 'policy framework', it will be necessary for the prosecution to lead evidence to prove this fact beyond reasonable doubt. As noted earlier, to do this, the prosecution may require proof that compromise of the information would be expected to cause serious or exceptionally grave damage to the national interest or other specified interests (a higher degree of harm than the harm required for s 122.2).

4.57 The CDPP advised that to prove that the information was security classified information they 'anticipate leading that evidence from a senior person in the relevant agency'.[189] Whether that person is able to provide the 'best evidence' as to the reasons for the original classification decision will depend to some extent on whether they made the decision and what records have been kept of the original decision-making.

4.58 If the defence were to challenge the original classification decision, there may be practical considerations that stem from it not being a requirement of the PSPF or agency practice that records be kept of the reasons a classification was selected for particular information or even when that decision was made or by whom (see **Annex D**).

4.59 Although it does not have any evidential value, the Attorney-General's certification as to classification is an important safeguard, but its operation is not straightforward either.

Attorney-General's certification

4.60 Under s 123.5(1) of the *Criminal Code*, proceedings for the commitment of a person for trial for an offence against Part 5.6 relating to security classified information must not be instituted without a certification by the Attorney-General that, at the time of the conduct that is alleged to constitute the offence, it was appropriate that the information had a security classification.

4.61 AGD stated, 'the requirement is an important feature of the operation of Part 5.6 that is intended to address concerns about the application of Part 5.6 to security classified information, such as the potential for incorrect classification of information'.[190]

---

188 See for example: The President of the United States, Classified National Security Information (Executive Order no 13526, 29 December 2009); *Reducing Over-Classification Act 2010* (US).

189 CDPP, *Submission 20*, 3.

190 AGD, *Submission 7*, 23 [107].

4.62 Both the Law Council of Australia and the Australian Human Rights Commission (AHRC) made submissions that, while the requirement for Attorney-General certification should be retained, it is insufficient protection and does not justify a broad deemed harm offence. The Law Council stated that 'primary reliance should not be placed on [consent and certification] as a safeguard because the proportionality of criminal offences should not be determined by the beneficial exercise of Ministerial discretion'.[191] Additional discussion on the role of consent and certification as safeguards is in **Chapter 10**.

4.63 Certification by the Attorney-General provides a check on the appropriateness of a classification, including by addressing the potential passage of time between the initial classification decision and the time at which the offence was committed. However, it is a final safeguard, not a substitute for proper systems, training and internal review of decision-making by officials. It is quite possible that the Attorney-General could find that some information, despite being in a document marked as secret or top secret, is not 'security classified information' within the meaning of s 90.5(1). This might be because of an error in the original classification decision in relation to that information, because of changes due to the passage of time or because the original classification decision was consistent with the 'policy framework' but that the relevant part of the policy framework was not consistent with the requirements of s 90.5(1)(a).

4.64 For information that the Attorney-General did certify as 'appropriately' classified, there is the possibility that *that* decision could be subject to a collateral challenge under s 75(v) of the Constitution. It is also not entirely clear if 'appropriate' classification means the same thing as 'in accordance with' the policy framework. It must also be remembered that the Attorney-General's certification needs to be in respect of information, not documents. Classification markings are generally applied to whole documents. Some documents may contain both information that is appropriately classified as secret or top secret as well as information that is of a lower classification or not classified (and thus not 'classified information' for the purposes of s 90.5). Some agencies apply a classification marking to each paragraph of some types of documents and then give the overall document a classification as well.

Technical and associated matters relating to security classified information

4.65 In addition to the uncertainty arising from the interaction between the *Criminal Code* and the PSPF, there are a number of more technical matters that add to the uncertainty of the meaning of security classified information, including:

- whether the reference to 'the policy framework' in s 90.5 is intended to refer to the PSPF, and if so, whether it is intended to refer only to the PSPF and the policies made

191 Law Council of Australia, *Submission 19*, 46 [167].

under it or also to other internal policies on security classification relied upon by staff in Commonwealth departments and agencies

- if the reference to the 'the policy framework' is intended to refer to the PSPF, whether it would it be interpreted by a court as the PSPF and accompanying policies as in force at a set point in time or as in force from time to time (and, if there is a prosecution, what version of the PSPF is to be relied upon to prove a security classification was applied in accordance with the PSPF)
- the way in which the definition of 'security classification' in s 90.5(1)(a)(i) refers to 'expected to cause serious damage to the *national interest*, *organisation or individuals*' for the classification of secret, whereas s 90.5(1)(a)(ii) refers to 'exceptionally grave damage to the *national interest*' for the classification of top secret
- uncertainty as to which parts of the PSPF must be adhered to in order for information to be 'classified in accordance with' that policy – for example, the PSPF is quite specific about things like the colour and placement of classification markings on physical documents and metadata requirements for electronic records.

4.66 Unlike the larger problems of uncertainty, accuracy and evidence discussed earlier, some of these 'technical matters' are capable of being addressed by relatively straightforward amendments. However, those which go to the policy framework being able to be amended at any time by the executive are connected to the much larger rule of law issue that arises as a result of decisions under a policy framework being incorporated into an element of an offence.

4.67 The rule of law issues are discussed next and the 'technical' matters are returned to at the end of security classified information section in this chapter.

Rule of law considerations

4.68 For all of the reasons discussed above, it is far from clear that incorporating the idea of security classifications applied under a policy framework brings any real certainty or clarity into the offence. But, even in cases where a classification decision was properly made under the correct policy framework and was consistent with s 90.5(1) and there was admissible evidence to prove beyond reasonable doubt that compromise of the information would be expected to cause serious or exceptionally grave damage to Australia's national interest, there are still fundamental rule of law concerns with incorporating decisions made under a policy into an element of a serious criminal offence.

Using a policy document to determine a key element of a crime

4.69 The joint academic submission described the rule of law as a 'set of principles [requiring] laws to be clear and accessible, for their administration to be as transparent as possible, and for their impacts to be proportionate and justified'.[192]

4.70 As explained in the Law Council's 'Rule of Law Principles', a key principle of the rule of law is that the law must be both readily knowable and available, as well as certain and clear. The effect of this for a criminal offence is that:

> [t]he intended scope and operation of offence provisions should be unambiguous and key terms should be defined. Offence provisions should not be so broadly drafted that they inadvertently capture a wide range of benign conduct and are thus overly dependent on police and prosecutorial discretion to determine, in practice, what type of conduct should or should not be subject to sanction.[193]

4.71 The joint academic submission stated that the use of the PSPF as an element of the deemed harm offence was a rule of law concern because 'the PSPF is an administrative document that can be changed without any involvement from parliament' and that it is 'inappropriate for an important aspect of a serious criminal offence to be set purely by administrative fiat'.[194] The HRLC similarly emphasised that it is 'not appropriate for a policy framework to dictate whether information has been applied the correct security classification' for the purposes of a criminal offence.[195] At the public hearing, the HRLC described the rule of law concerns as follows:

> The Human Rights Law Centre has two rule of law concerns having a policy document … govern serious criminal offences. … [First,] that the law should be both readily known and available and certain and clear. And this means that people must clearly know that their actions might give rise to a civil or criminal penalty, and also that any action undertaken by the executive should be authorised by law. …
> Secondly, … a policy document is not subject to that same level of scrutiny and public accountability as legislation. … [The] rule of law require that any subordinate legislation is … subject to that parliamentary oversight.[196]

4.72 The Law Council of Australia was equally strongly opposed 'to the approach of referring to administrative instruments, that may be subject to variation from time to time and are not subject to parliamentary scrutiny, to define key definitional concepts about a serious indictable offence'.[197]

---

192 Joint Academic Submission, *Submission 13*, 4.
193 Law Council of Australia, *Rule of Law Principles* (Policy Statement, March 2011) 2.
194 Joint Academic Submission, *Submission 13*, 9.
195 Human Rights Law Centre (HRLC), *Submission 14*, 12.
196 Ms Olivia Roney, HRLC, *Public hearing transcript*, 25 March 2024, 21.
197 Law Council of Australia, *Submission 19*, 19 [43].

4.73 The counterargument to saying that s 122.1 does not meet rule of law requirements because it leaves an essential element to policy is that the requirement in s 90.5(1)(a)(i)–(ii) provides some certainty because the policy framework for identifying information as secret or top secret must be consistent with those requirements.

4.74 It may be accepted that, by including a definition of what a secret and top secret classification means within the text of the statute, s 90.5(1)(a)(i) and (ii) do impose some restrictions on what the policy framework can say. As discussed in this chapter, there are already some differences between the *Criminal Code* and the policy framework, with the likely consequence that some information will not be 'security classified' for the purpose of the *Criminal Code* even if it is marked as secret or top secret. The guidance in s 90.5(1)(a)(i) and (ii) is skeletal. Concepts in the statutory text such as the 'national interest' are broad and susceptible to the risk that these terms will be applied by reference to any policy set out in the PSPF and associated documentation.

4.75 In other words, incorporating decisions made under a 'policy framework' into a core element of a criminal offence is inconsistent with the rule of law because it does not provide sufficient 'certainty'. This is partly because of how uncertain the application of the policy framework is but more fundamentally because of the way that the executive can change the effect of the law at any time by changing the policy without any parliamentary control. Section 90.5(1)(a) provides some mitigation but it insufficient because it leaves too much discretion to the executive in setting the boundaries of an offence. There is an additional rule of law concern related to 'knowability' which I turn to next.

Using a document that is not publicly available to determine when a classifcation is to be applied

4.76 In addition to the general rule of law concerns discussed above, there is a specific concern that arises because not all parts of the 'policy framework' are publicly available – and thus it cannot be truly 'knowable' and 'available' for a person to assess whether a classification has been applied *in accordance with* the policy framework, an essential element of the law.

4.77 PSPF Policy 8 contains many requirements that officials are obliged to comply with. One of them is 'requirement 6', which states:

> *Requirement 6 mandates that caveated information and accountable material be clearly marked and handled in accordance with the originator and the caveat holder's special handling requirements as established in the Australian Government Security Caveats Guidelines. These special caveat requirements apply in addition to the classification handling requirements. Additional information about handling caveats is available in the Sensitive Material Security Management Protocol and the Australian Government Security Caveats Guidelines on a need to-know basis on GovTEAMS.*[198]

198 *PSPF Policy 8* (n 161) 11 [47].

4.78 This requirement seems to mean that officials are to comply with the Sensitive Material Security Management Protocol and the Caveat Guidelines, neither of which is publicly available.

4.79 At the public hearing, the Department of Home Affairs (which has policy responsibility for the PSPF) was asked whether there were any classified annexes or other policies that form part of PSPF Policy 8. The department took this question on notice and later provided advice that the Caveat Guidelines have to be applied:[199]

> **Question:**
> [Can you confirm] that the version of Policy 8 publicly available on the PSPF website is the full and complete version and there are no classified annexes or other policies that are not publicly available which are relevant in determining whether a classification is 'in accordance with' the PSPF for the purposes of section 90.5.
>
> **Answer:**
> The Department confirms this is correct, unless the classified material has a security caveat applied, then the classified Australian Government Security Caveat Guidelines would also apply.[200]

4.80 The Department of Home Affairs later said in an email that the 'additional protections [in the Caveat Guidelines] do not affect the classification of a document, but in some cases, may change how the documents are handled. All policy relating to classification are publicly available'.[201]

4.81 I have been provided with a copy of the Caveat Guidelines. It is around 40 pages long and also has an annex which is more highly classified. The Caveat Guidelines and annex describe a number of code words and caveats and when they are to be applied, as well as special handling requirements for material so marked. They have a very brief description of when each code word or caveat is to be applied and specify what security classification is to be applied to information given that code word or caveat.[202]

4.82 Examples of the descriptions of when a code word or caveat is to be applied include:

> [code word] is applied to all references to [agency], locations, operations and capabilities.

---

199 Mr Nathan Smyth, Home Affairs, *Public hearing transcript*, 25 March 2024, 74–75.
200 Home Affairs, *Supplementary response 25*.
201 Email from Home Affairs to the INSLM, 17 April 2024.
202 There are also instructions specific to some which require that additional 'warning' text be included on any documents containing the material and in some cases that additional administrative measures are to be taken to restrict who has access to the material.

> [and]
>
> Details of the application of the [redacted] caveat are classified; however ASD's intelligence functions are outlined in unclassified terms in section 7 of the *Intelligence Services Act 2001*.[203]

4.83 For anything marked with the code word or caveat in those examples, the policy requires that the material must be classified as secret or top secret and additional administrative measures are to be applied.

4.84 Some caveats and code words are applied to foreign governments' information where that information is provided to Australia. In accordance with the Caveat Guidelines and annex, those code words and the corresponding security classification of secret or top secret must also be automatically applied to the information and other information derived from it.

4.85 The 'assessing whether information is security classified' flowchart in PSPF Policy 8 requires an assessment of whether the information should be classified as top secret, secret or protected (in that order). Then, if it is 'caveated information not already captured' by one of those classifications, it must be 'classified as at least protected'.[204]

4.86 The policy is not particularly clear. It is easy to see how some caveats and code words could be applied to broad classes of information under the Caveat Guidelines. A result of this is that a marking of secret or top secret would then be applied. This has a practical consequence that the individual assessments that that disclosure would likely cause the serious or exceptionally grave damage to Australia's national interest that s 90.5(1)(a) appears to require is not made out. As a result it is likely that at least some of the information would not meet the test in s 90.5(1)(a) and would, as such, not be 'classified information' regardless of what is stamped on it. But aside from this practical problem there is also a more fundamental rule of law problem with using a document such as the Caveat Guidelines and its annex – which are not publicly available – as part of a policy framework which is incorporated into the criminal law.

4.87 I find that at present the full 'policy framework' under which information is actually determined to be 'security classified information' includes policies which are not publicly available (and, indeed, some of those cannot be made publicly available because they are

---

203 *Australian Government Security Caveat Guidelines* 13 (Guideline, 28 July 2022) ('*Caveat Guidelines*').

204 *PSPF Policy 8* (n 161) 9.

themselves classified). A law cannot be 'knowable' in the rule of law sense if it is not entirely publicly available.[205]

4.88 The conclusion that classification decisions are made based on the Caveat Guidelines is consistent with advice received from one of the intelligence agencies, which told this review in its initial submission that 'All [agency] information is classified, at minimum, as SECRET in accordance with the Australian Government Protective Security Policy Framework'.[206] In response to questions on notice, the agency confirmed that this requirement is based on the Caveat Guidelines and annex.[207]

4.89 This result raises self-evident rule of law concerns. It is also questionable whether the Caveat Guidelines and annex are consistent with s 90.5(1)(i)–(ii) of the *Criminal Code* because they require the application of a caveat and a classification for reasons that are not expressly linked to the types of damage described in those paragraphs, including situations where a foreign partner has applied a caveat or code word under their own policies.

International law concerns

4.90 In addition to the rule of law concerns and concerns about how classifications operate in practice, there were submissions about international law focused on consistency with art 19 of the ICCPR. These are related to the rule of law concerns about the role of a policy document in describing elements criminal law.

4.91 The principal international law concern that the AHRC raised was consistency with art 19(2) of the *International Covenant on Civil and Political Rights* (ICCPR), which protects freedom of expression. Article 19(3) provides that rights provided for in art 19(2) may be subject to restrictions that are provided *by law* and are necessary including for the protection of national security (see **Chapter 3**).

4.92 AHRC stated in its written submission:

> While there may be guidelines produced by the Executive from time to time about how … security classifications are to be applied, the Commission considers that it is not appropriate for the 'Protective Security Policy Framework', to be a determinant of an element of a serious

---

205 As noted earlier, in practice, many officials will make decisions based on internal policies that are not publicly available. If these are considered part of the Commonwealth's framework then the same issue arises.

206 Classified submission to INSLM Review of Part 5.6 of the *Criminal Code*, 1 March 2024.

207 Classified response to questions on notice, INSLM Review of Part 5.6 of the *Criminal Code*, 16 April 2024. Note that the agency also advised that on 3 April 2024 it decided to commence a review of its application of the code word, noting that in some corporate circumstances it may no longer be as necessary to use such a code word.

> offence. Setting the parameters of a criminal offence by reference to policy or guidelines, which can be changed at any time without Parliamentary oversight or a mechanism for disallowance, is inconsistent with Australia's international obligations.[208]

4.93 The Human Rights Commissioner expanded on these submissions in evidence at the public hearing:

> **MS LORRAINE FINLAY**: … [The PSPF] framework as a policy document, [that] can be subject to change with little notice, with little transparency, and without full parliamentary oversight. And in our view, that raises concerns … with freedom of expression obligations that Australia has under the *International Covenant on Civil and Political Rights*.
>
> …
>
> **MS FINLAY**: [I]n addition to being necessary and proportionate, the requirement under article 19 is that, of course, any restrictions be made by law. And one of the difficulties in terms of having a policy document that is changeable and that can be changed without full parliamentary oversight and without that level of transparency and accountability, is you do call into question that fundamental requirement of being made by law, which, as we've mentioned, really does highlight the interrelationship between freedom of expression and the rule of law as human rights obligations. …
>
> **MS JANE FRASER**: … I would [add] that the things that limit the right must be accessible to the public and must provide sufficient guidance both to those executing the laws and those whose conduct is being regulated. So the limitations need to be as provided by law.
>
> …
>
> **MS FINLAY**: … And in terms of a strong encapsulation of those requirements under article 19, we'd certainly refer you to general comment No. 34 by … the Human Rights Committee … which in particular at paragraph 22 does highlight, of course, that there can be restrictions, but does acknowledge that 'provided by law' criteria as being the first criteria that must be applied in terms of any applicable restrictions.[209]

4.94 The AHRC's submissions and evidence highlight a key concern with the incorporation of the PSPF as an element of the offence in s 122.1 for Australia's international obligations: it may not be consistent with the requirement in art 19(3) of the ICCPR that any restriction to the right of freedom of expression must be 'provided by law'. Guidance on art 19(3) is provided in the United Nations Human Rights Committee (UNHCR) *General Comment No. 34 on Article 19: Freedoms of Opinion and Expression* (UN General Comment 34), which states:

> For the purposes of [art 19(3)], a norm, to be characterized as a 'law', must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly and it must be made accessible to the public. … Laws must provide sufficient guidance to those

---

208 Australian Human Rights Commission (AHRC), *Submission 17*, 16 [57].

209 *Public hearing transcript*, 25 March 2024, 33.

> charged with their execution to enable them to ascertain what sorts of expression are properly restricted and what sorts are not.[210]

4.95 The use of the PSPF as an element of the deemed harm offence relating to security classified information may not be consistent with the requirement in art 19(3) of the ICCPR that any restriction to the right to freedom of expression must be 'provided by law' because the PSPF is a policy document that may be changed by the executive at any time without public and parliamentary scrutiny. The fact that, as discussed above, documents associated with the PSPF which also guide classification decision-making are not publicly available increases the likelihood that the current approach is not consistent with Australia's international obligations under the ICCPR. See also **Chapter 3**.

Security classified information and recklessness

4.96 In contrast to the various concerns raised about the inclusion of security classified information, AGD said that one of the benefits is:

> [It enables the prosecution to] provide evidence that a defendant was reckless as to harm where the harm has been properly assessed by the originator of the information in accordance with the requirements of the Protective Security Policy Framework (PSPF) and communicated to the defendant through the application of a TOP SECRET or SECRET security classification marking.[211]

4.97 There was concern that removing the reference to classification in the offence would make it more difficult to prove recklessness.

4.98 In related comments, the Law Council of Australia emphasised that recklessness is not required to be established for at least one aspect of the offence because it is 'strict liability'. The Law Council considered that strict liability should be removed from the offence. They point out that strict liability is generally only justified when requiring proof of fault would diminish deterrence and 'there are legitimate grounds for penalising persons lacking "fault" in respect of that element'. The Law Council is particularly concerned about the use of strict liability in relation to security classification because it depends on an administrative instrument (the PSPF) that can be changed at any time and is not subject to parliamentary scrutiny.[212]

---

210 United Nations Human Rights Committee (UNHCR), *General Comment No. 34 on Article 19: Freedoms of opinion and* expression, 102nd sess, UN Doc CCPR/C/GC/34 (12 September 2011) [25] ('*UN General Comment 34*').

211 AGD, *Submission 7*, 10 [45].

212 Law Council of Australia, *Supplementary submission 26*, 21.

4.99 Before addressing these concerns, it is necessary to briefly explain how recklessness operates in relation to classification-based offences and what is meant by strict liability. 'Recklessness' is defined in s 5.4 of the *Criminal Code*:

> **5.4 Recklessness**
>
> (1) A person is reckless with respect to a circumstance if:
>
> (a) he or she is aware of **a substantial risk that the circumstance exists** or will exist; and
>
> (b) **having regard to the circumstances known to him or her, it is unjustifiable to take the risk**.
>
> (2) A person is reckless with respect to a result if:
>
> (a) he or she is aware of a substantial risk that the result will occur; and
>
> (b) having regard to the circumstances known to him or her, it is unjustifiable to take the risk.
>
> (3) The question whether taking a risk is unjustifiable is one of fact.
>
> (4) If recklessness is a fault element for a physical element of an offence, proof of intention, knowledge or recklessness will satisfy that fault element.
>
> [Emphasis added.]

4.100 Under s 6.1(2) of the *Criminal Code*, if a law that creates an offence provides that strict liability applies to a particular physical element of the offence, there are no fault elements for that physical element and the defence of mistake of fact is available. For an offence involving strict liability, the defence of mistake of fact applies where, at or before the time of the conduct constituting the physical element, the person considered whether or not facts existed, and is under a mistaken but reasonable belief about those facts, and had those facts existed the conduct would not have constituted the offence (see *Criminal Code*, s 9.2(1)).

4.101 As discussed earlier in this chapter, there is complexity and uncertainty in proving the physical element that information is 'security classified information' – that is, that the information has been classified as secret or top secret in accordance with the relevant policy framework. There is also considerable complexity in the fault (mental) element, which seems to have aspects of both strict liability and recklessness. Strict liability has a nuanced application in relation to security classified information.

4.102 Section 121.1(3)(a) of the *Criminal Code* provides that strict liability applies to the element of the offence that 'a classification is applied in accordance with the policy framework developed by the Commonwealth for the purpose of … identifying the information mentioned in subparagraph 90.5(1)(a)(i) or (ii)' (see also s 90.5(1A)(a)). The consequence of applying strict liability to the element of security classification seems to be that it is not necessary for the prosecution to prove that a person was *reckless* as to whether information was classified *in accordance with* the PSPF. However, it may still be necessary for the prosecution to prove that a person was reckless as to whether information was in fact classified 'secret' or 'top secret'.

4.103 The Supplementary Explanatory Memorandum to the EFI Bill described the rationale for the application of strict liability as follows:

> Strict liability is appropriate for this element of the definition because the person's state of mind about the fact that the classification was applied under an appropriate Commonwealth policy framework for the purpose of identifying such information is not relevant to their culpability. It is sufficient for the prosecution to prove that the person was reckless as to the fact that the information was classified as SECRET or TOP SECRET. It is not reasonable to expect that a person would be familiar with the methods for applying classifications to information, nor the exact meaning of the classifications. There is unlikely to be sufficient evidence to allow the prosecution to prove that a person was reckless about this level of detail about the policy framework sitting behind the application of a classification of SECRET or TOP SECRET[213]

4.104 The CDPP's view is:

> [Section] 121.1(3) of the Criminal Code … provides that strict liability applies to the element of an offence that the security classification has been applied in accordance with the policy framework. The strict liability in relation to that element applies only to the accused's state of mind. That is, the prosecution does not have to prove the accused's intention, knowledge, recklessness or negligence in relation to whether the policy framework was applied. The prosecution still has to prove the fact that the information was classified in accordance with the policy framework.[214]

4.105 Assuming that the prosecution is required to establish that the person was reckless as to the fact that the information was classified (as opposed to whether it was *correctly* classified), this might be able to be proved by establishing that the person had seen the classification markings on a document containing the information in question and that their training and experience was such that they recognised the marking as a classification marking of secret or top secret.

4.106 It may be accepted that recklessness may be more difficult to prove, at least in some cases, if it is necessary to establish recklessness in relation to the *nature* of information rather than whether it has a security classification. It will be necessary to establish the nature of the information if other parts of the definition of inherently harmful information are relied on (these are discussed later in this chapter). However, discussion with CDPP suggests that, while it will always depend on the particular facts and circumstances, the following matters

213 Supplementary Explanatory Memorandum, National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2018 (Cth) 16 [40] ('*EFI Bill*').

214 Email from CDPP to INSLM, 27 March 2024.

will probably be relevant to proving an individual's state of mind in relation to inherently harmful information of *any* type:

- the layout of a document containing the information and the markings on it – for example, a document with headings or other markings which describe it as an intelligence report or intelligence assessment
- classification markings on a document, particularly if there are code words or other markings which indicate it came from a particular agency or source
- where the document was accessed – for example, whether it was downloaded from an intelligence agency system
- the individual person's experience and training in the use of classification markings and code words and in seeing intelligence reports and the way they are laid out
- any training or briefings the individual might have had to complete to gain access to the system the information came from
- the actual content of the document containing the information – although to rely on this aspect it would probably also be necessary to establish that the person had read the document.

4.107 Most of these points will apply to either establishing that the person was reckless as to whether a document contained classified information or to whether a document contained intelligence information (see discussion below on the second part of the definition of inherently harmful information), so the actual evidence to be led will be similar.

4.108 CDPP also noted that, to prove the fault (mental) element of recklessness, all the available evidence, including subjective matters relevant to the individual, must be assessed. For example, the fact that an individual is the holder of a security clearance and has undertaken training on the PSPF is likely to be relevant in assessing that individual's state of mind in relation to security classified information.

4.109 I accept AGD's concern that in some cases it may be more difficult to establish recklessness without the current element of strict liability for security classified information. However, this does not outweigh all the reasons concerning uncertainty, rule of law and compliance with international obligations discussed above. Furthermore, classification markings and other design elements of documents will still be relevant to determining whether a person is reckless as to the proposed elements of the offence as revised by the recommendations made later in this chapter.

Findings and recommendations on security classified information

4.110 Relying on classification markings to guide how officials use, store and disseminate information is a longstanding and reasonable approach to protecting sensitive information within government agencies. However, seeking to incorporate a classification policy directly into the criminal law raises many legal and practical issues. There is real uncertainty about how a court would interpret and apply the definition of classified information. A likely outcome is that proof would be required to the criminal standard that the information had been properly classified. Evidence would need to be led that disclosure would cause serious damage to the national interest or grave damage to the national interest – higher thresholds than the harm-based offence in s 122.2. Inconsistency between some classification policies and procedures and the requirements of the *Criminal Code* mean that some documents marked as secret or top secret may not in fact be 'classified information' for the purposes of the offence even if the official who made the classification decision followed those policies. Current procedures for the system of classification decision-making, including training, guidance material and record keeping, is not set up to support decisions being made to the criminal standard.

4.111 Moreover, there is a fundamental rule of law issue with having as a core element of an offence decisions made under a policy framework that can be changed at any time and is not all publicly available. Furthermore, use of a policy document to frame a criminal offence may not meet Australia's international obligations, including that limits on freedom of communication be imposed *by law*.

4.112 Certification by the Attorney-General that a classification is appropriate is an important safeguard and should be retained if this recommendation is not accepted. However, certification is a final safeguard and should not be relied on to remedy all of the other problems with incorporating a policy framework into a criminal law. The fact that the certification decision may be subject to collateral challenge in a prosecution also risks bringing more complexity and more sensitive information into what could already be a very complex prosecution.

4.113 Removing classification markings as a physical element of the offences does not mean that they have no role to play whatsoever. A classification marking combined with evidence of an official's training and experience in what those markings indicate would go a long way towards establishing, as matter of fact, the required mental element of recklessness to a risk of harm.

4.114 Lastly, I note a recent example of prosecution for the disclosure of classified documents that did not require a specific 'classified information' offence such as that in s 122.1. In the case

of *R v McBride (No 4)*[215] Mr Mc Bride was convicted of theft contrary to s 131.1(1) of the *Criminal Code* as well as communicating naval, military or air force information contrary to s 73A(1) of the *Defence Act 1903*.[216] Central to the case was the removal and subsequent disclosure of 235 documents from ADF facilities, 207 of which were marked as 'secret'.[217]

RECOMMENDATION 1: The offences in Part 5.6 should not rely on information being classified under a policy framework as an element of the offence.

Technical matters associated with security classification

4.115 As noted earlier, there are also some 'technical matters' associated with incorporating the PSPF into statute. Unlike the fundamental rule of law and uncertainty issues, some of the technical matters may be able to be resolved by amendments. However, these do not need to be addressed if **Recommendation 1** is accepted and their resolution will not remove the greater concerns which led to that recommendation.

Whether 'the policy framework' in section 90.5 is intended to refer to the PSPF

4.116 The phrase 'the policy framework' in s 90.5 is not defined in the *Criminal Code*. The Explanatory Memorandum to the EFI Bill indicates that it is intended to refer to the PSPF and the policies made under it.[218] The Department of Home Affairs gave evidence that this was their understanding.[219] The analysis earlier in this chapter proceeded on the basis that this was correct. However, this is not certain, and it is not inconceivable that the 'policy framework' for the purposes of s 90.5 could change or be significantly amended. This would lead to even greater uncertainty in the operation of the offence. To promote further certainty and clarity, the phrase 'the policy framework developed by the Commonwealth' should be defined more clearly.

4.117 Even if this phrase is defined more clearly, a further issue may need to be addressed: whether, on the assumption that the reference to the 'policy framework' is intended to refer to the PSPF, it is limited to the PSPF or also extends to other policies on security classifications of 'secret' and 'top secret' that Commonwealth departments and agencies rely on. Some of these policies, discussed in this chapter, are expressly described in the PSPF as being mandatory for officials to apply – including the Caveat Guidelines. It is also possible that other policies not referred to in the PSPF may be taken to form part of the 'policy framework' for

215 [2024] ACTSC 147.
216 All relevant actions occurred before the enactment of Part 5.6 of the *Criminal Code*.
217 [2024] ACTSC 147 [43].
218 Revised Explanatory Memorandum, EFI Bill (n 213) [511], [521], [523].
219 Home Affairs, *Supplementary response 25*.

the purpose of s 90.5, depending on whether the Commonwealth has developed those policies to identify information as secret or top secret. It should be clear on the face of the legislation exactly what policies form part of the 'policy framework' that is referred to in s 90.5. Also, all of those policies should be publicly available or at least accessible to those who are subject to an offence that relies on security classification (which currently means everyone, because of the use of security classifications in the offence for non-officials in s 122.4A). It would be better if they were in the form of a disallowable legislative instrument to provide a level of parliamentary scrutiny if they are to be part of the criminal law.

Whether 'the policy framework' is intended to refer to the PSPF at a specific point in time or from time to time

4.118 On the assumption that the reference to the 'policy framework' in s 90.5 is intended to refer to the PSPF, there is significant uncertainty as to whether the reference to the 'policy framework' is the policy framework at a set point in time or as in force from time to time.

4.119 On the one hand, there is a common law principle of statutory interpretation that, in the absence of a clear statutory indication to the contrary, it is assumed the law is what parliament made it at the time an Act is enacted. Therefore, any document incorporated into the law is assumed to be incorporated as it was at the time the relevant law was made.[220] That said, the purpose and context of the reference to the PSPF – that is, to prevent the disclosure of security classified material – arguably provides a statutory indication to the contrary. It would arguably best achieve this purpose for the reference to the PSPF to be read as meaning the PSPF as in force at the time that the information was classified. How a court would resolve this is unclear.

4.120 However, even if a court accepted that there was a clear intention to override the common law presumption, this leaves questions as to what happens if the PSPF has changed in a material way between the time of classification and when the disclosure or 'dealing with' occurred. For example, is it the version of the PSPF at the time Part 5.6 was enacted, the time that the information was classified or the time of the conduct that is alleged to constitute the offence (or some combination of each or all of these)? There may also be difficulties in identifying and proving the correct version of relevant documents, depending on the administrative mechanisms in place in relevant agencies for version control of amendments

220 See eg, *Forsyth v Deputy Commissioner of Taxation* (2007) 231 CLR 531; Pearce and Geddes, *Statutory Interpretation in Australia* (LexisNexis Butterworths, 8th ed, 2014) [6.22]. Section 46AA of the *Acts Interpretation Act 1901* (Cth) modifies the common law when legislation authorises or requires provision to be made in relation to any matter in an instrument, other than a legislative instrument, a notifiable instrument or a rule of court. However, it is not clear that the reference to a 'policy framework' is a reference to an 'instrument' so it is not clear that s 46AA applies. If it did apply then s 46AA(2) means the instrument cannot incorporate matters in an instrument or other writing as in force from time to time except for provision in Acts, legislative instruments and rules of court.

particulalry if the decision was based on a Guideline or internal policy. All of this reinforces that much greater clarity is needed for the definition and operation of the the defined term 'security classified information' in s 90.5 of the *Criminal Code* if security classification is to be retained as an element of the deemed harm offence.

4.121 If the common law presumption is displaced and parliament's intention is that it is the PSPF as amended from time to time that is being referred to, this reinforces the rule of law concerns discussed above – in particular, the concern that the reference to the 'policy framework' in s 90.5 means that the executive can incorporate future changes to the framework into the criminal law without parliamentary scrutiny.

Classified information – national interest versus organisations and individuals

4.122 As mentioned above, for the classification of 'secret', the definition of 'security classification' in s 90.5(1)(a)(i) uses the phrase 'expected to cause serious damage to the *national interest*, *organisations or individuals*' (emphasis added). However, for the classification of 'top secret', s 90.5(1)(a)(ii) refers to 'exceptionally grave damage to the *national interest*' (emphasis added). In other words, top secret information is limited to grave damage to the national interest, whereas secret information extends to serious damage to the national interest, organisations or individuals.

4.123 Given the seriousness of the offences that turn on these definitions, it is appropriate that both of the definitions be limited to the *national interest*. Harms to the health or safety of the Australian public or a section of the Australian public are separately covered in the definition of 'cause harm to Australis's interests' in ss 122.2 and 122.4A.

4.124 The lack of any definition of 'national interest' leaves significant uncertainty as to how this phrase will be interpreted.

Classified information – which parts of the policy framework are mandatory?

4.125 There is also some uncertainty about how much of the PSPF needs to be applied correctly if information is to be proved beyond reasonable doubt to have had a classification *applied in accordance with* that framework. In addition to the classification decision being based on the harm that unauthorised disclosure could be expected to cause, the PSPF is quite specific about things like the colour and placement of classification markings on physical documents and metadata requirements for electronic records.[221] It is not clear if the reference to a 'classification applied in accordance with the PSPF' means merely whether the *level of classification* has been applied in accordance with the PSPF or whether it extends to other requirements relating to the classification, such as markings.

---

221 *PSPF Policy 8* (n 161) Annex A, 29.

Information connected to a domestic or foreign intelligence agency

4.126 I have dealt comprehensively with why 'security classifications' under a policy framework should not form an element of a criminal offence. I now turn to the second part of the definition of 'inherently harmful' information, which is broadly about intelligence agency information. In practice, most intelligence agency information will be marked as secret or top secret, but this element of the offence does not depend on classification; it depends on whether the information was 'information that was obtained by, or made by or on behalf of, a domestic intelligence agency or a foreign intelligence agency in connection with the agency's functions'.[222]

4.127 The term 'domestic intelligence agency' is defined in s 121.1(1) to mean:

(a) the Australian Secret Intelligence Service; or
(b) the Australian Security Intelligence Organisation; or
(c) the Australian Geospatial-Intelligence Organisation; or
(d) the Defence Intelligence Organisation; or
(e) the Australian Signals Directorate; or
(f) the Office of National Intelligence.

4.128 Although these agencies are not specifically defined in the *Criminal Code*, a court would probably identify the agencies and their functions having regard to their relevant statutes under which they are established (that is, the *Australian Security Intelligence Organisation Act 1979* (Cth) (*ASIO Act*), the *Intelligence Services Act 2001* (Cth) (*IS Act*) and the *Office of National Intelligence Act 2018* (*ONI Act*). Unlike the other 5 agencies, which all have specified statutory functions, the Defence Intelligence Organisation (DIO) is an administrative part of the Department of Defence and does not have defined statutory functions.[223]

4.129 The definition of 'inherently harmful information' in s 121.1(1)(c) also refers to information that was obtained or made by or on behalf of a 'foreign intelligence agency'. 'Foreign intelligence agency' is defined in the Dictionary of the *Criminal Code*:

> ***foreign intelligence agency*** means an intelligence or security service (however described) of a foreign country.

4.130 It should be noted that intelligence information that a domestic intelligence agency obtained in confidence from a foreign intelligence agency would already be covered by the earlier part of the definition (as intelligence information obtained by a domestic intelligence agency).

---

222 *Criminal Code* (n 157) s 121.1(1)(c).

223 Note that the functions of ASIS can be extended by directions given by the ASIS Minister: see *Intelligence Services Act 2001* (Cth) s 6(1)(e) ('*IS Act*'). Those directions are not publicly available.

Therefore, it does not appear necessary, or appropriate, to refer to foreign intelligence agencies separately. Put another way, given that information obtained by a domestic intelligence agency from a foreign intelligence agency would already be covered by the offence in s 122.1, it is not necessary or appropriate for the offence to separately cover information obtained or made by or on behalf of a foreign intelligence agency. None of the comparable Five Eyes laws include this type of language, and there does not appear to be any compelling reason for Australian law to criminalise the disclosure of information of a foreign intelligence agency unless it has been shared with or produced in collaboration with an Australian agency.

All information connected to intelligence agencies

4.131 The central issue arising in the review concerning the deemed harm offence relating to domestic intelligence agency information is whether it is necessary and proportionate for the offence to apply to *all* information obtained or made by or on behalf of an intelligence agency in connection with *any* of the agency's functions.

4.132 AGD provided the following policy explanation for why the offence was originally drafted to include all information about all functions:

> a reason for including all information obtained by, or made on behalf of, a domestic or foreign intelligence agency was to address concerns that unauthorised disclosures of even small amounts of information could, when taken together with other information, compromise national security, regardless of the apparent sensitivity of the particular information. In addition, information that relates to any operations or functions of an intelligence agency will often be highly sensitive as an intelligence agency's corporate functions are integral to its intelligence functions.[224]

4.133 Intelligence agencies also made submissions in favour of maintaining the broad deemed harm offence over all intelligence agency information. Conversely, in submissions and evidence, non-government groups expressed a range of concerns about the inclusion of all intelligence agency information in the deemed harm offence.

4.134 In the discussion below, I set out the key intelligence agency submissions in support of the current approach and then discuss the key concerns about the breadth of the current offence. I then consider whether it is possible to identify a narrower category of intelligence agency information. Finally, I discuss concerns about information obtained in connection with DIO's functions being included in the deemed harm offence when those functions are not set by parliament.

224 AGD, *Submission 7*, 12 [55].

Breadth of the offence

4.135 As noted above, the deemed harm offence relating to intelligence agency information applies to all information obtained or made by a domestic or foreign intelligence agency, regardless of whether the information was obtained or made in the exercise of an intelligence function.

4.136 In support of the present offence, the Australian Signals Directorate (ASD) submission stated:

> Information concerning the operations, capabilities, technologies and methods used by intelligence agencies is sensitive, and can be used by adversaries to gain an advantage, or circumvent protective measures agencies provide to Australia.
>
> ASD considers it impossible to definitively state that harm was not caused by the unauthorised communication of sensitive information, as the ramifications of disclosure include elements that cannot be easily quantified.
>
> Additionally, information which may appear innocuous could, when viewed in aggregate and alongside publicly available information, be used by foreign intelligence services to gain access to or disrupt ASD business or reveal the details of covert targets, capability or methods used by ASD ...[225]

4.137 It is an unusual proposition to suggest that it is appropriate to make something a serious crime because it is not possible to establish that harm was not caused by the action.

4.138 ONI stated:

> Dividing intelligence agency information into [categories of 'intelligence' and non-'intelligence' information] would inevitably result in speculation and guesswork by potential disclosers, who would form their view based on incomplete information about the equities inherent in the material they are considering disclosing.
>
> 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.[226]

4.139 The reason that 'mosaic analysis' does not sit easily with criminal culpability has already been discussed in **Chapter 2**. In short, this is because criminal offences have a physical and a fault (mental) element, and requiring an individual to have knowledge of the impact of disclosure of information based on the mosaic effect (including the way in which information may be

225 ASD, *Submission 4*, 5 [12]–[13].
226 ONI, *Submission 8*, 2–3.

used by foreign adversaries) is not something that is not necessarily knowable, especially by an outsider. The criminal law does not ordinarily attach criminal culpability to consequences that an individual cannot foresee and which are entirely outside their control.

4.140 ONI's submission also supported retaining all information relating to any intelligence agency within the deemed harm offence on the basis that changing this may impact the security culture in government:

> **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. Downplaying this level of harm creates real risks of undermining whole-of government information security culture.[227]

4.141 Managing 'security culture' is ultimately a matter of policy and leadership, with most sanctions being administrative in nature (see **Chapter 1**). While the criminal law has a role to play, there is no reason this should not be through a combination of deemed harm and harm-based offences.

4.142 The Australian Secret Intelligence Service (ASIS) submission focused on the ASIS-specific offences in the *IS Act* but said that ASIS requires the 'high[est] levels of secrecy about its activities, operations, targets, capabilities, methodologies, locations, and personnel'.[228] This list is a subset of the information currently covered by the current category of *any* information obtained or made by or on behalf of an intelligence agency in connection with *any* of the agency's functions.

4.143 The Australian Security Intelligence Organisation (ASIO) took a nuanced view to which types of information require inclusion in a deemed harm offence and which can potentially be adequately protected by harm-based offences. ASIO said that the highest level of protections are required for:

a. ASIO's operations, subjects of ASIO inquiries and investigations, capabilities, technologies, methods, and human sources – and those of our partners;
b. vetting (particularly Top Secret) information – both personal information about clearance applicants and clearance holders, and the vetting standard and derivative processes and policies used to undertake vetting; and
c. the identities of ASIO employees and affiliates, including information about our employees and affiliates that could be exploited by foreign intelligence services.[229]

227 ONI, *Submission 8*, 3 (emphasis in original).
228 ASIS, *Submission 10*, 4 [19].
229 ASIO, *Submission 6*, 4 [19].

4.144 In evidence at the public hearing, the Director-General of Security expanded on the reason a subset of ASIO information requires particular protection:

> [T]here is a narrow set of circumstances where particularly sensitive information cannot be publicly disclosed in a parliament, court or the media. As Justice Hope said, and I quote: 'a large measure of secrecy is essential for the effective performance of ASIO's security intelligence function. ASIO has to be able to protect sources and methods, and in some circumstances, results of its operations. Personal information that ASIO may need to collect in the course of its work requires protection in the interests of the privacy of the individuals concerned'. … ASIO acknowledges the public's right to information. However, this must be balanced against the need to prevent disclosure that could severely damage national security, national interest, and put people's safety at risk. …[230]

4.145 The Director-General of Security also gave evidence to the effect that disclosure of a range of administrative, staffing and procurement activities *may* result in harm in some instances but that not all such disclosures will (except the identity of ASIO staff and affiliates).[231] It is worth noting that, of the intelligence agencies, ASIO is the one with the most experience at defending its decisions in proceedings, including decisions involving an assessment that harm may result from an action. For example, ASIO is regularly called upon to defend its Adverse Security Assessments (in broad terms, these are assessments of security risks relating to a particular person) in merits and judicial review proceedings before Commonwealth courts and tribunals. As noted by the Director-General in his evidence, it has generally been successful in doing so.[232]

All information 'obtained by, or made on behalf of' an intelligence agency is a very broad category

4.146 As noted in the Issues Paper, information obtained by or made on behalf of a domestic intelligence agency or a foreign intelligence agency 'in connection with the agency's functions' in s 121.1(1)(c) would potentially be given a broad meaning based on what little judicial consideration there has been of similar wording in other offences.[233] A similar formulation in the *IS Act* was considered in *R v Collaery (No 12)*[234] in the context of a subpoena where the judge said it did not require that the Crown prove that the disclosure involved only activities that were 'within' the functions of the intelligence under any applicable legislation or that each of the requirements of such legislation was complied with in relation to those activities. If that is correct then this aspect of the definition covers an

230 Mr Mike Burgess, Director-General of Security, *Public hearing transcript,* 25 March 2024, 10.
231 Mr Mike Burgess, Director-General of Security, *Public hearing transcript,* 25 March 2024, 15–16.
232 Mr Mike Burgess, Director-General of Security, *Public hearing transcript,* 25 March 2024, 14.
233 *INSLM Issues Paper* (n 156) 41 [2.40].
234 [2022] ACTSC 108 [13].

extremely broad category of information, including potentially information that was not lawfully obtained by the agency in the first instance.

4.147 It is uncontroversial that some information obtained or made by or on behalf of a domestic intelligence agency in connection with the agency's functions would cause harm if publicly disclosed. For example, disclosing the name of a current ASIS operative or source operating overseas would clearly cause a serious risk of arrest or other harm to that person. Disclosing the target of current foreign intelligence collection activities would be likely to prejudice that particular operation, as well as cause damage to Australia's international relations and intelligence collection capabilities. Similarly, disclosing details of current technology that intelligence agencies use for lawful electronic surveillance which would allow that surveillance to be avoided would clearly cause harm to those intelligence capabilities. However, it does not necessarily follow that *everything* that was obtained or made by or on behalf of a domestic intelligence agency in connection with the agency's functions would cause harm if the information was disclosed publicly.

4.148 A similar point was made by a former INSLM's review of a deemed harm offence in s 35P of the *ASIO Act*:

> My examination of the operation of the [special intelligence operation] (SIO) scheme in practice confirms that risks of the kind outlined are real in relation to certain (perhaps most) kinds of intelligence operations with certain (perhaps most) kinds of authorised illegal behaviour. It does not follow that the same risks will be inherent in relation to all information relating to all SIOs for all time. The rationale for the width of the section depends on harm, of the kind outlined, being implicit in any disclosure of any information about an SIO at any time. That is simply not sustainable.[235]

4.149 The offence in s 122.1 is much broader that the one considered in that INSLM review. Section 35P applies only to ASIO Special Intelligence Operations, while s 122.1 applies to any information obtained by or made by or on behalf of any intelligence agency in connection with its functions.

4.150 The Law Council of Australia's submission argued that the phrase 'in connection with the agency's functions' does not provide a sufficiently precise definition to demarcate the boundaries of what may be a serious indictable criminal offence.[236] I agree with this and would add that, in addition to lacking precision, it is also disproportionately broad in capturing a range of information that lacks a necessary or sufficient connection to harm. In managing their affairs, all of the intelligence agencies make or obtain information not directly connected to covert operations. This includes a range of information that is not protected from disclosure in other agencies – for example, information relating to personnel management and procurement. As a hypothetical example, evidence of sexual harassment,

---

235 *INSLM Report on Section 35P of the ASIO Act* (n 140) 22 [41].

236 Law Council of Australia, *Submission 19*, 24 [64].

procurement fraud or maladministration in ASD, DIO or the Australian Geospatial-Intelligence Organisation (AGO) would appear to fall within the scope of the deemed harm offence, even if the disclosure did not include information about operations or capabilities and was not likely to cause any harm to national security or defence. In contrast, the same information about another part of the Defence could be disclosed publicly.[237] The deemed harm offence relating to intelligence agency information is also not limited by time, so disclosures of information that may once have been harmful but are no longer harmful are penalised in the same way as harmful disclosures.

Agency functions have expanded

4.151 The breadth of the offence is underscored by the expansion in intelligence agency functions over the past 15 years.

4.152 In its 2009 Secrecy Laws Report, the ALRC said that intelligence agencies were in a special category when it comes to secrecy offences and that this may justify the inclusion of intelligence information in a deemed harm offence. This finding was made before the expansion of intelligence agency functions, including into less traditional areas. For example, since 2009:

- AGO has been given functions to enable it to assist Commonwealth and State authorities that are engaged in emergency response functions, safety functions, scientific research functions, economic development functions, cultural functions and environmental protection functions, as well as expanded scope to assist the Australian Defence Force (ADF).[238] AGO has also become the Australian Hydrographic Office mentioned in s 223 of the *Navigation Act 2012* (Cth) (which includes some commercial mapping functions).[239]
- ASD has been given a function of preventing and disrupting, by electronic or similar means, cybercrime undertaken by people or organisations outside Australia.[240] Further, ASD's information security function has greatly expanded in scope (it was previously limited to advising government bodies and now includes a wide range of non-government entities).[241]

---

237 The information could be disclosed to the IGIS in accordance with the public interest disclosure scheme, but that alone does not mean that it should be a crime to disclose non-harmful information publicly or that deemed harm offences should be excessively broad.

238 *IS Act* (n 223) s 6B(1)(ea)–(g).

239 *IS Act* (n 223) s 6B(3)–(4).

240 *IS Act* (n 223) s 7(1)(c).

241 *IS Act* (n 223) s 7(1)(ca), (2).

- ASIS has been given an express function of providing assistance to the ADF in support of military operations and to cooperate with the Defence Force on intelligence matters.[242]
- ONI has been given an express function to collect 'open source' intelligence as well as expanded functions relating to the evaluation and coordination of the intelligence community.[243]
- All of the intelligence agencies have been given the function of assisting each other and any agency prescribed by the Regulations with the performance of their functions.[244]

It is not possible to assess changes in DIO's functions since 2009, as the DIO mandate was not made publicly available until after 2019.

4.153 Since the *EFI Act* was enacted in 2018, the domestic intelligence agencies have further expanded in both size and functions:

- ONI and ASIO both have additional functions in relation security vetting.[245]
- The widest expansion has arguably been the extension of ASD's functions, using the regulations-making power, to include assisting the Department of Home Affairs with the performance of any of the department's functions.[246]

4.154 This means that the deemed harm secrecy offence in s 122.1 now applies to any information obtained by, or made by or on behalf of, ASD while it is assisting the Department of Home Affairs. The Department of Home Affairs is a department of state with a very wide range of policy and operational roles. One hypothetical example might be where ASD makes a translator available to assist with an immigration interview. If the ASD staff member disclosed a record of that interview, they would be subject to the deemed harm offence in s 122.1. However, if a Department of Home Affairs staff member disclosed a record of that same interview, they would not. A similar situation would arise if ASD provided staff with cybersecurity expertise to assist the Department of Home Affairs in the development of a cybersecurity strategy or policy. It is difficult to see any sound reason why information about ASD assistance with these functions should *automatically* fall within a 7–10-year deemed

242 *IS Act* (n 223) s 6(1)(ba).

243 *Office of National Intelligence Act 2018* (Cth) s 7 ('*ONI Act*'). The former *ONI Act – Office of National Assessments Act 1977* (Cth) – included a general function of 'to assemble and correlate information relating to international matters that are of political, strategic or economic significance to Australia': see s 5(1)(a).

244 *IS Act* (n 223) s 13A and *Australian Security Intelligence Organisation Act 1979* (Cth) s 19A ('*ASIO Act*'); *ONI Act* (n 243) s 14.

245 *ONI Act* (n 243) s 7(1)(ba) and *ASIO Act* (n 244) s 17(1)(cb).

246 *IS Act* (n 223) s 13; *Intelligence Services Regulations 2021* (Cth) reg 5.

harm offence and why it cannot be adequately covered by the general harm-based offences in s 122.2 and s 122.4 that would also apply to information about the department.

May not comply with international law obligations

4.155 Another issue to be considered is whether, particularly in light of their expanded functions, it is 'necessary' in the international law sense of the term for the deemed harm offence to apply to all intelligence agency information.

4.156 As already discussed in **Chapter 3,** under art 19(3) of the ICCPR, restrictions to the right to freedom of expression must be 'necessary' for a legitimate purpose. As outlined by the UNHRC in *UN General Comment 34*, restrictions must not be 'overbroad'. They must:

- conform to the principle of proportionality
- be appropriate to achieve their protective function
- be the least intrusive instrument amongst those which might achieve their protective function
- be proportionate to the interest to be protected.

4.157 The AHRC stated that criminalising all information made or obtained in connection with a domestic intelligence agency's functions is neither necessary nor proportionate to achieve the legitimate objective of national security.[247]

4.158 There is a real question as to whether it is consistent with this obligation for all information obtained by, or made by or on behalf of, a domestic or foreign intelligence agency to be included in a deemed harm offence. This is particularly because there is a narrower category of intelligence-related information that will probably always be harmful if disclosed which could be described for a deemed harm offence. Other information about intelligence agencies can be covered by a harm-based offence.

Intelligence information

4.159 One of the questions posed in the Issues Paper was:

> Should all information that was obtained by, or made by, a domestic or foreign intelligence agency in connection with that agency's functions be part of a 'deemed harm' offence or is there only a subset of this information which it is reasonable and proportionate to cover with a 'no harm' offence?[248]

4.160 Having considered the submissions, including intelligence agency submissions, I made the following statement at the start of the public hearings:

---

247 AHRC, *Submission 17*, 14 [50].

248 *INSLM Issues Paper* (n 156) 41–44 [2.39]–[2.50] and 46, issue 16.

> Most independent reviews in the past have said that deemed harm offences should be reserved for the narrowest category possible of information – things that are always harmful. My preliminary view is that the strongest argument for a class of information which might be justified as inherently harmful is that which relates to the core intelligence gathering functions of these agencies. For ASD, AGO and ASIS, and possibly DIO, this could be described as things that relate to the operations, capabilities, methods, or sources used to obtain intelligence information a term that's already defined in their legislation. A similar thing could potentially be said in relation to ASIO for security intelligence and perhaps its new vetting function. And it may be that the argument for deemed harm offences is strongest in the case of current and former intelligence officials themselves.[249]

4.161 Each of the intelligence agencies was asked about this proposal during the hearings and had the opportunity to make supplementary submissions. While supplementary submissions were received from others on this issue, none were made by intelligence agencies.

4.162 Following discussions with AGD, I refined the proposal put forward at the public hearing to expressly include within a proposed amended deemed harm offence intelligence information itself as well as the operations, capabilities, technologies, methods and sources used to obtain or communicate that information. Intelligence information, operations, capabilities, technologies, methods and sources that foreign partners provide to Australia would also be covered by this category. Disclosure of specific types of intelligence information and operations (etc.) will always, or almost always, result in harm to the national interest. There are other aspects of the work of intelligence agencies and other agencies with intelligence functions the disclosure of which *may* harm the national interest. These are appropriately covered by harm-based offences discussed in **Chapter 5** and **7**.

4.163 'Intelligence information' is a term already defined in the *IS Act*:

> ***intelligence information*** means the following:
>
> (a) intelligence obtained by ASIS under subsection 6(1) 6(1) (other than intelligence obtained solely under paragraph 6(1)(da));
>
> (c) intelligence obtained by AGO under paragraph 6B(1)(a), (b) or (c);
>
> (d) intelligence obtained by ASD under paragraph 7(1)(a);
>
> (ca) intelligence obtained or produced by DIO in the performance of its intelligence functions;
>
> (e) incidentally obtained intelligence.

4.164 In broad terms, the definition includes intelligence obtained in the performance of particular functions (that is, those relating specifically to the collection of intelligence), as well as incidentally obtained intelligence but not information that was obtained solely in the performance of other functions or information that is administrative in nature.

---

249 Mr Jake Blight, INSLM, *Public hearing transcript*, 25 March 2024, 7.

4.165 It is not a new concept that some information that intelligence agencies generate under specific functions is 'intelligence information' while other information is not. ASIS, ASD, AGO and DIO are already required to identify 'intelligence information' (as defined in the *IS Act* for each agency) in their possession in order to apply rules to protect the privacy of Australians.[250] For example, at the hearing ASD gave evidence that they are able to identify intelligence information, including by the way the information was obtained.[251] This reinforces my view that, for the purpose of a deemed harm offence, it is possible in practice to distinguish between information that agencies obtain for their intelligence functions and information they obtain for their other functions.

4.166 It should be acknowledged that many of the additional functions of intelligence agencies, particularly for ASD and AGO, may involve the use of capabilities and technologies that are *also* used for the production of intelligence information. For example, ASD might theoretically use a capability that was primarily designed to obtain foreign intelligence information in order to undertake its cybercrime disruption or cybersecurity function. Information that concerns the operations, capabilities, technologies, methods and sources used to obtain or communicate intelligence information is still information of that character, even if those capabilities (etc.) are also used for other non-intelligence purposes. Nevertheless, it is the result, and my intention, that some information, including about cybersecurity and mapping capabilities, will no longer be *automatically* covered by the deemed harm offence. Where disclosure of that information is likely to lead to harm, the harm-based offence in s 122.2 or s 122.4 will continue to apply (**Chapter 5** and **8**).

4.167 For ASIS there would be little change, as the definition of 'intelligence information' for ASIS in the *IS Act* includes information that ASIS has obtained pursuant to all of its functions, apart from information obtained *solely* to assist another agency with the performance of the other agency's functions. Given the breadth of ASIS's primary functions, it would seem very rare that this would arise. If it did arise then, as in the examples of ASD assisting the Department of Home Affairs with translating or policy development discussed above, such a circumstance would not warrant the automatic application of a 7–10-year deemed harm offence. As discussed later in this chapter, I have recommended retaining the specific offence relating to the disclosure of the identity of a current or former ASIS staff member or agent. Any other information that ASIS has obtained or made that was *solely* connected to assisting another agency with its functions may be covered by the harm-based offence in s 122.2 (if its disclosure will or is likely to cause relevant kinds of harm) or, if the other agency is itself a domestic intelligence agency, may be covered by s 122.1 if it is intelligence information of that agency.

250 *IS Act* (n 223) ss 15 and 41C.

251 Mr Stephen McGlynn, ASD, *Public hearing transcript*, 25 March 2024, 65–66.

4.168 The definition of 'intelligence information' in the *IS Act* does not refer to ASIO. ASIO's core intelligence collection and analysis functions are described in s 17(1)(a) the *ASIO Act* as 'intelligence relevant to security'. This is a very broad security intelligence function because the definition of 'security' in the *ASIO Act* is so broad. Nevertheless, ASIO's primary intelligence function is clearly tied to the definition of 'security' and there is a sound argument that 'intelligence information' for ASIO should include all of this information. In accordance with s 17(1)(e) of the *ASIO Act* ASIO also has a specific foreign intelligence function that should also be covered by the deemed harm offence.

4.169 After careful consideration I have recommended that ASIO's functions relating to assessing and granting the highest level of security clearances (see s 17(1)(cb) and Part IVA of the *ASIO Act*) should not be the subject of the general deemed harm offence in s 122.1. However, that information should be included in a specific offence in the *ASIO Act* (**Recommendation 4**). The reasons for this are discussed later in this chapter.

4.170 ONI's functions are set out in s 7 of the *ONI Act*. They include to assemble, correlate and analyse information relating to particular matters of significance to Australia and to prepare assessments and reports in relation to such matters (s 7(1)(c) and (d)). ONI also has a specific function that concerns the collection of what it calls 'open source' intelligence. This is the only function to which ONI's privacy rules apply.[252] ONI also has functions that concern the preparation of what can be called strategic intelligence assessments.[253] It is reasonable to assume that the covert operations, capabilities, technologies, methods and sources used for these 2 sets of functions and the intelligence outputs are the types of intelligence functions that will always or almost always result in harm to the national interest.

4.171 The function in s 7(1)(e) of the *ONI Act* of giving the Prime Minister advice on intelligence requirements and capabilities can similarly be accepted to involve information that will always or almost always result in harm to the national interest for the purpose of s 122.1.

4.172 The remainder of ONI's functions relate to leadership and evaluation. While they are no doubt sensitive, they are the types of activities for which a harm-based offence is more suitable. The harm-based offence in s 122.2 would also continue to apply to broadly similar activities relating to security, defence or international relations undertaken by other agencies, including the Department of Defence, the Department of the Prime Minister and Cabinet and the Department of Home Affairs.

4.173 For DIO the definition of 'intelligence information' in the *IS Act* is rather circular: intelligence information is 'intelligence obtained or produced by DIO in the performance of its intelligence

252 *ONI Act* (n 243) ss 7(1)(g), 53.

253 *ONI Act* (n 243) s 7(1)(c) and (d). Communication of those reports under s 7(1)(i) would be covered.

function'. From the language in the policy document that currently describes DIO's 'mandate', it is not entirely obvious which of its functions are its 'intelligence functions'.[254] If DIO's functions are put on a statutory footing, the types of functions that are 'intelligence functions' could be made much clearer. For the reasons discussed further at the end of this chapter I have recommended DIO's functions be put on a statutory footing.

4.174 The Law Council of Australia made a supplementary submission which gave in-principle support to the above proposal to narrow the deemed harm offence in respect of its application to intelligence information.[255] The Law Council's supplementary submission also recommended a number of other changes to further limit the deemed harm offence.[256]

Findings and recommendations on intelligence agency information

4.175 Deemed harm offences should only be used for information that is always, or almost always, going to be harmful to a critical national interest if disclosed. The actual core intelligence operations, capabilities, technologies, methods and sources of Australia's 6 main intelligence agencies fall into this category. But it does not follow that *all* information to do with those agencies will always be harmful. This is particularly so for agencies whose functions have expanded beyond traditional intelligence functions. The same is true for routine administrative and corporate functions – disclosure of information about non-intelligence functions and administrative activities *can* result in harm in *some* circumstances but not with the degree of certainty that justifies a deemed harm offence. Where these other activities cause harm or are likely to cause harm including to security, defence or international relations, they will continue to be covered by the harm-based offence in s 122.2 (see **Recommendation 6**). There are also grounds for continuing the special protections afforded to the identities of ASIS and ASIO staff and agents (see **Recommendation 4**).

4.176 The deemed harm offence relating to intelligence agency information should be narrowed to cover intelligence information, as well as the methods, capabilities, technologies, methods and sources used to obtain that information. For ASIS, ASD and AGO 'intelligence information' should be defined by reference to the existing definition of 'intelligence information' in the *IS Act*. For ASIO, it should cover information relevant to security under s 17(1)(a) of the *ASIO Act*, as well as ASIO's foreign intelligence function in s 17(1)(e) of that Act. For ONI, the definition of 'intelligence information' should be linked to ONI's statutory intelligence functions in s 7(1)(c), (d), (e) and (g) of the *ONI Act*. It is intended that the deemed

254 Also see Lieutenant General Gavan Reynolds, DIG, *Public hearing transcript*, 25 March 2024, 71–72.
255 Law Council of Australia, *Supplementary submission 26*, 2.
256 Law Council of Australia, *Supplementary submission 26.*

harm offence only apply to covert operations, capabilities, technologies, methods and sources.

4.177 Consistently with the current offence, intelligence information that foreign partners share with intelligence agencies in confidence, as well as the methods, capabilities, technologies, methods and sources used to obtain that information, should be covered by the offence and would appear to already fall within the proposed definition of 'intelligence information'.

4.178 For this offence to apply to DIO, **Recommendation 5** would need to be accepted and DIO's functions would need to be put on a statutory footing. In that process, DIO's intelligence functions should be expressly identified in the *IS Act* in a way similar to those of ASD, AGO and ASIS.

RECOMMENDATION 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.

Information relating to a domestic or foreign law enforcement agency

4.179 The third part of the definition of 'inherently harmful information' in s 121.1(1)(e) covers all 'information relating to the operations, capabilities or technologies of, or methods or sources used by, a domestic or foreign law enforcement agency'. There is no definition of a 'domestic or foreign law enforcement agency' in the *Criminal Code*. In other statutory contexts, 'law enforcement agency' has been held to extend to any authority or person whose responsibilities include the enforcement of a law or laws of the Commonwealth or a State – for example, the CDPP, the Australian Criminal Intelligence Commission (ACIC), Australian Securities and Investments Commission and the Australian Taxation Office (ATO).[257] In addition, s 121.1(1)(e) does not require that a disclosure about a domestic law enforcement agency be about current operations (etc.) or that a disclosure about a foreign law enforcement agency have any impact on Australia.

4.180 Further, there is no requirement that information 'relating to' operations (etc.) actually prejudice or harm any 'operations, capabilities or technologies of, or methods or sources'. No doubt there is a lot of information which, if disclosed, would prejudice the operations, capabilities, technologies, methods or sources used by a domestic or foreign law

257 See eg, *Australian Crime Commission v AA Pty Ltd* (2006) 149 FCR 540, [23], [34].

enforcement agency. However, it does not necessarily follow that *all* information 'relating to' those topics is prejudicial or that it remains prejudicial for an indefinite period of time or equally for all agencies. Also, it does not follow that a deemed harm offence is the most appropriate way to deal with any prejudice to the criminal justice system that may be caused as a result of a disclosure.

A broad category of law enforcement information

4.181 In its submission to this review, AGD explained the justification for including all information 'relating to the operations, capabilities, technologies, methods or sources used by a domestic or foreign law enforcement agency' in the deemed harm offence by reference to the Explanatory Memorandum to the EFI Bill:

> The framing of [the definition of 'inherently harmful information' in s 121.1(e)] captures all information relating to the operations, capabilities and technologies of, and methods and sources used by, a law enforcement agency. … [I]nformation that falls into one or more of these categories has the potential to prejudice investigations and operations, and, as is the case in the disclosure of information concerning human sources or officers operating under assumed identities, compromise people's safety. Law enforcement agencies possess sensitive information about capabilities and operations, which can have profound national security implications, including information on counter terrorism, espionage and foreign interference, covert services, human sources and organised crime. With law enforcement increasingly dealing with or leading responses to national security threats such as these, the risks associated with the unauthorised disclosure of law enforcement information are likely to increase.[258]

4.182 The Department of Home Affairs noted growing interaction and overlap between law enforcement and national security, saying:

> law enforcement can fall under the umbrella of national security – making law enforcement inherently tied to national security information. To treat them differently would be separating aspects of national security, contrary to the holistic approach necessary to defend Australia and its interests.
>
> … For example the ABF (within the Department) provides information (gathered incidentally to their law enforcement functions) to intelligence agencies supporting NIC capability. NIC agencies also provide intelligence to law enforcement for purposes of supporting law enforcement activities. Therefore, the Department submits that law enforcement agency information requires robust protection, akin to that of national security classified information.[259]

4.183 Some law enforcement agencies, particularly the Australian Federal Police (AFP), are involved with national security matters, including counterterrorism and foreign interference.

258 AGD, *Submission 7*, 13 [59].
259 Home Affairs, *Submission 2*, 9.

However, this is clearly not the case for all agencies whose operations would be captured by the current offences. As discussed above, in other contexts the phrase 'law enforcement agency' has been held to include any agency whose responsibilities include the enforcement of a law. For example, the Great Barrier Reef Marine Park Authority may be considered a 'law enforcement agency' because it can appoint inspectors who have powers of search and entry of aircraft, vessels and premises. Many other agencies could be similarly covered by the current offence.

4.184 AGD stated that an additional consideration in the framing of s 121.1(1)(e) was that some agencies, such as the ACIC, have both law enforcement and intelligence functions and that any definition of 'law enforcement agency' should not restrict the ability of agencies with both law enforcement and intelligence functions from relying on the general secrecy offences in Part 5.6 of the *Criminal Code*.[260] AGD said that any attempt to define the specific subtypes of information relating to the operations, capabilities, technologies, methods and sources of a law enforcement agency in a way that removes these subtypes of information from the offence risks removing from the offence information that would cause genuine harm if disclosed without authorisation.[261]

4.185 The current approach of casting the offence in extremely wide terms was the primary concern raised in submissions to the review.

4.186 Referring to breadth of the deemed harm offence relating to law enforcement information, AHRC said that, while some information in the category may be harmful at some times, it does not follow that all information in this category would cause harm if publicly disclosed.[262]

4.187 The Law Council of Australia expressed its concerns about the deemed harm offence relating to law enforcement in terms of a lack of precision, which also contributed to concerns about breadth:

> In principle, the Law Council does not consider that 'information relating to the operations, capabilities or technologies of, or methods or sources used by, a domestic or foreign law enforcement agency' is a sufficiently precise demarcation of a category of information where disclosure is inherently associated with harm. Because there is no requirement that information 'relating to' operations etc. actually prejudice or harm any 'operations, capabilities or technologies of, or methods or sources', the Law Council submits that this category of information is more proportionately addressed in the context of a general secrecy offence that is subject to an express harm requirement. As the INSLM's Issues Paper notes,

260 AGD, *Submission 7*, 13 [61].
261 AGD, *Submission 7*, 13–14 [62].
262 AHRC, *Submission 17*, 14 [48].

> 'it does not necessarily follow that all information 'relating to' those topics is prejudicial or that it remains prejudicial for an indefinite period of time'.[263]

4.188 A further concern raised was the difficulties caused for the application of the offence by the absence of a definition of 'law enforcement agency' in Part 5.6 of the Criminal Code. In particular, the AFP and AUSTRAC reported difficulties with applying the deemed harm offence relating to law enforcement information in the absence of a definition of 'law enforcement agency'.[264] The Law Council also submitted that the lack of a definition of 'law enforcement agency' in the *Criminal Code* results in uncertainty about the scope of the deemed harm offence.[265]

A cascading approach to law enforcement information

4.189 Law enforcement information is gathered to investigate and prevent crime but also with a view to obtaining admissible evidence that can be used to prosecute a criminal offence – a role that intelligence agencies generally do not have.[266] Some law enforcement activities may have an 'intelligence-only' purpose and some may rely on sensitive capabilities. But it is a large leap from there to saying *all* law enforcement information should be treated in the same way as the kinds of intelligence agency information or capabilities discussed earlier in this chapter. It is true that some agencies, including AFP, work closely with ASIO and others on counterterrorism and foreign interference and that these are highly sensitive operations. But, again, it does not follow that, as a result of that cooperation, *all* law enforcement information should be treated as though it was generated by ASIO or another intelligence agency.

4.190 It should also be noted that information a law enforcement official discloses that relates to ASIO's (or another intelligence agency's) *intelligence information* or the operations, capabilities, technologies, methods and sources used to obtain or communicate that information will already be covered by the offence in s 122.1 under **Recommendation 2**. For example, this would include information from a joint ASIO/AFP counterterrorism operation.

---

263 Law Council of Australia, *Submission 19*, 26 [69].

264 Australian Federal Police, *Submission 18*, 7; AUSTRAC, *Submission 15*, 5.

265 Law Council of Australia, *Submission 19*, 26 [71]–[73].

266 For example, s 11(2) of the *IS Act* (n 223) makes clear that ASIS, ASD and AGO do not have 'police functions' or 'any other responsibility for the enforcement of the law'. However s 11(2) also makes clear that this does not prevent the agencies from passing intelligence relevant to crime to law enforcement authorities or from assisting law enforcement authorities with there functions were prescribed in the regulations (as is the case with ASD and Home Affairs) or from performing specific law enforcement related or assistance functions in s7(1)(c)(e) and 6B(1)(e)(ea).

4.191 It is not necessary or proportionate for *all* information relating to the operations, capabilities, technologies, methods or sources of a domestic of foreign law enforcement agency to be covered by a 7–10-year deemed harm offence.

4.192 However, this does not mean that the disclosure of information that would undermine law enforcement operations, capabilities, technologies, methods and sources does not deserve sanction. It is appropriate for a cascading approach to be taken to offences relating to the disclosure of law enforcement information in the secrecy offences in Part 5.6 of the *Criminal Code*. I suggest that this approach involve 3 tiers of law enforcement information: first, the most sensitive types of law enforcement information relating to electronic surveillance technologies, capabilities and methods (which should be covered by the deemed harm offence in s 122.1); second, information that may cause harm to other capabilities granted by parliament to agencies to investigate criminal offences through the exercise of statutory powers (which should be covered by the 7–10-year harm-based offence in s 122.2); and, third, any other information that prejudices the prevention, detection, investigation, prosecution or punishment of a criminal offence against any law of the Commonwealth which falls within the general 2-year harm-based offence in s 122.4.

Electronic surveillance capabilities

4.193 The first tier of law enforcement information (falling within the deemed harm offence) should be limited to the technologies, capabilities and methods that support the extraordinary electronic surveillance powers granted to a small number of law enforcement agencies to combat serious crimes. Examples include electronic surveillance powers granted to law enforcement agencies under the *Telecommunications (Interception and Access) Act 1979* (*TIA Act*), *Surveillance Devices Act 2004* (*SD Act*) and the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (*SLAID Act*). Part 2-5 of the *TIA Act* provides for law enforcement agencies to apply to eligible judges and tribunal members for telecommunications service and named person warrants to authorise the interception of telecommunications. The *SD Act* provides for law enforcement officers to apply for surveillance device warrants and computer access warrants authorising the use of surveillance devices and enabling access to data held on computers. The *SLAID Act* amended the *SD Act*, *Crimes Act 1914* (Cth) and associated legislation to introduce new powers for the AFP and ACIC, including data disruption warrants, network activity warrants and account takeover warrants.

4.194 Each of these extraordinary electronic surveillance and disruption powers can be viewed as equivalent, at least in terms of information sensitivity, to the technologies, capabilities and methods that intelligence agencies use in the exercise of their intelligence collection functions. The technology needed to use these covert powers requires significant investment. If the technology and related methodology are compromised, they would take a long time to replace and law enforcement agencies' ability to combat serious and organised

crime would be seriously undermined. Electronic surveillance capabilities used by law enforcement agencies are in a special category similar to intelligence agency covert collection capabilities and sources in that disclosure of information about the capability can be expected to always, or almost always, cause significant and long-term damage to law enforcement agencies' ability to combat serious crime using extraordinary powers granted by parliament. Therefore, it is reasonable for information that would undermine this narrow category of capabilities to be covered in a deemed harm offence.

4.195 It is logical that a person who is providing information about a criminal undertaking or organisation will always, or almost always, be at real risk of harm if their identity is disclosed. More broadly, it is clear that the disclosure of the identity of a covert human source will have flow-on effects on the ability to recruit covert human sources in future. Therefore, consideration could also be given to including disclosure of the identity of a covert human source in this aspect of the deemed harm offence if it can be shown that offences including those associated with witness protection, assumed identity and controlled operations are not sufficient. The issue of covert human sources was raised by the AFP late in this review. I agree in principle that, if there is a genuine 'gap' in the protection of covert human sources and if it is possible to clearly identify what is mean by a 'covert human source', a deemed harm offence may be appropriate but this issue was not explored in detail in any submissions to this review.

Other statutory powers and prejudice to criminal investigations

4.196 The second tier of law enforcement information (which should fall within the 7–10-year harm-based offence in s 122.2) is information the disclosure of which may undermine the utility of capabilities used to investigate crime by police or other law enforcement agencies under statutory powers. This category of law enforcement information should include capabilities connected to statutory powers to access information or to search people, places or things including covert forensic tools used to analyse electronic devices seized under a search warrant. It would also include search and seizure powers that have been granted to a wide range of agencies; and other powers to require the production of information in order to combat crime. It is not appropriate to include information relating to the exercise of these statutory powers in the deemed harm offence because the disclosure of this information *may* (but not always or almost always) cause significant harm to law enforcement capabilities. Some is the type of information that is often disclosed in prosecutions and some is not covert. In cases where the capability would be compromised by disclosure, it is reasonable to expect that evidence of harm can be established without the same kinds of difficulties that may arise in seeking to establish harm for sensitive intelligence collection and law enforcement electronic surveillance capabilities. This 'tier' is discussed further in **Chapter 5**.

4.197 The third tier of law enforcement information should be that which the ALRC originally proposed be included in a general harm-based offence: information the disclosure of which

may prejudice the prevention, detection, investigation or prosecution of a criminal offence against any law of the Commonwealth. This broad category of information should fall within the general harm-based offence in s 122.4, regardless of which agency is involved. It does not involve a need to establish that the disclosure undermined a particular capability or was connected to a statutory power. This offence, combined with a range of existing specific offences such as those relating to perverting the course of justice, witness protection, assumed identities and obstructing officials, are directed at the overall integrity of the criminal justice process. This is discussed further in **Chapter 7**.

Findings and recommendations on law enforcement information

4.198 There should be some type of sanction for intentional or reckless interference with the integrity of the criminal justice system or disclosures that undermine law enforcement capabilities. However, it does not follow that all of these should be covered equally by same deemed harm offence. This review recommends a cascading approach. The serious deemed harm offence in s 122.1 should apply only to the technologies, capabilities and methods that support the extraordinary electronic surveillance powers that parliament has granted a small number of agencies to combat serious crimes. Other capabilities that support statutory crime fighting powers should be covered by the harm-based offence in s 122.2. The general offence in s 122.4 should have broader application to cover other types of prejudice to the operation of the criminal justice system. These 3 offences, combined with a range of existing specific offences such as those relating to perverting the course of justice, witness protection, assumed identities and obstructing officials, are a proportionate response to the varied types of harm that can arise from unauthorised communication or dealing with law enforcement information.

RECOMMENDATION 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.

Similar offences in IS Act, ASIO Act and ONI Act

4.199 In addition to the general secrecy offences in Part 5.6 of the *Criminal Code*, ASIS, ASIO, ASD, AGO, DIO and ONI are subject to specific secrecy offences in the *IS Act*, *ASIO Act* and *ONI Act*. Section 39 of the *IS Act* relevantly prohibit the communication, recording or dealing with of information or records acquired or prepared by or on behalf of ASIS, AGO, ASD and DIO in connection with or related to the performance of their functions. Sections 18–18B of the *ASIO Act* prohibit the communication, dealing with or recording of information or records

acquired or prepared by or on behalf of ASIO in connection with or that relate to the performance of ASIO's functions. Sections 42 and 44 of the *ONI Act* prohibit the communication or dealing with of information or records made or obtained by or on behalf of ONI in connection with or that relate to the performance of ONI's functions.

4.200 The specific secrecy offences relating to ASIS, ASIO, ASD, AGO, DIO and ONI broadly apply to all information made or obtained by or on behalf of these agencies in connection with or that relate to the exercise of their statutory functions. Therefore, the concerns and reasoning about the deemed harm offence relating to intelligence information discussed in the Issues Paper and above apply to them as well. Similarly, the concerns about the inclusion of DIO's functions as a boundary of an offence when DIO's functions are not described in legislation (discussed in the Issues Paper and later in this chapter) also apply.

4.201 In 2019 the *Report of the Comprehensive Review of the Legal Framework of the National Intelligence Community* (Comprehensive Review Report) recommended the consolidation of the secrecy offences relating to ASIS, ASD, AGO and DIO in ss 39–40M of the *IS Act* without any expansion to those offences.[267] The reason given by the Comprehensive Review Report was that consolidating the offences would increase protection of ASIS identities by removing the specific reference to each agency thereby reducing the ability to identify whether it was an ASIS officer or agent who had been charged. The Comprehensive Review Report did not engage with questions about the necessity or proportionality of the breadth of the offences discussed above, nor with the problem of having DIO's undefined functions connected to a criminal offence (discussed later in this chapter).

4.202 During the course of this INSLM review the PJCIS inquired into the National Security Legislation Amendment (Comprehensive Review and Other Measures No. 3) Bill 2023. That Bill proposed, amongst other things, consolidating the secrecy offences as recommended by the Comprehensive Review in 2019. In its 21 March 2024 report on the Bill, the PJCIS recommended that the government consider aligning the proposed amendments to the *IS Act* and *ASIO Act* secrecy offences with recommendations that may be relevant from this INSLM review, pending the timing of the completion of that review and passage of the legislation.[268] The Bill proceeded to second reading on the first day of the next sitting period (14 May), passing the House that day and the Senate the next day.

4.203 Given the urgency with which the *National Security Legislation Amendment (Comprehensive Review and Other Measures No. 3) Act 2023* (*Comprehensive Review Act #3*) was enacted

---

267 National Security Legislation Amendment (Comprehensive Review and Other Measures No. 3) Bill 2023 (Cth) sch 2, pt 2; Dennis Richardson, *Comprehensive Review of the Legal Framework of the National Intelligence Community* (Final Report, December 2019) vol 3, 117, recommendation 143 ('*2019 Comprehensive Review*').

268 PJCIS, *Advisory Report on the National Security Legislation Amendment (Comprehensive Review and Other Measures No. 3) Bill 2023* (Report, March 2024) 26 [3.19], recommendation 4.

there was not time for this INSLM review report to be considered before its passage. Nevertheless, as the intelligence agency specific offences are closely related to Part 5.6 of the *Criminal Code* I did consider them in the course of this review and they are discussed in the following section of this report.

Deemed harm offences in IS Act, ASIO Act and ONI Act

4.204 The Issues Paper raised the question of whether the secrecy offences for the 6 main intelligence agencies should be in the *Criminal Code* rather than replicated in the *IS Act*, *ASIO Act* and *ONI Act*, noting the significant overlap between those offences and the offences in s 122.1 of the Criminal Code. Reducing the overall number of secrecy offences is a key goal of the AGD Secrecy Review.

4.205 AGD and the Department of Home Affairs,[269] and each of ASIS, ASIO, ASD, AGO, DIO and ONI, supported retaining the specific secrecy offences in the *IS Act*, *ASIO Act* and *ONI Act* in addition to the secrecy offences in the *Criminal Code*.[270]

4.206 AGD explained its position by reference to the principles for framing secrecy offences recommended in the AGD Review of Secrecy Provisions. Principle 2 provides that criminal liability for the protection of Commonwealth information should primarily be imposed through general secrecy offences in the *Criminal Code*.[271] Principle 3 provides that specific secrecy offences should only apply where criminal liability differs in significant and justifiable ways from general secrecy offences.[272] The primary justification the department offers for retaining the secrecy offences in the *IS Act*, *ASIO Act* and *ONI Act* is that 'there are significant differences in criminal liability between Part 5.6 of the *Criminal Code* and the specific secrecy offences in the [*IS Act*], [*ASIO Act*] and [*ONI Act]*, including differences in defences and penalties'.[273]

4.207 The reasons the intelligence agencies gave for preferring to retain offences in their own Acts were broadly similar. They included the following:

- The offences in the *ASIO Act*, *IS Act* and *ONI Act* apply to a limited category of people and there are differences in maximum penalties and defences as compared to the *Criminal Code* offences.
- The Comprehensive Review Report did not recommend repealing the specific secrecy offences in the *IS Act*, *ASIO Act* and *ONI Act*. Instead, it favoured a

269 AGD, *Submission 7*, 9–10 [40]–[42]; Home Affairs, *Submission 2*, 8.

270 ASIS, *Submission 10*, 6–9 [29]–[49]; ASIO, *Submission 6*, 5–6 [27]–[30]; ASD, *Submission 4*, 3–4 [5]–[9]; DIG, *Submission 5*, 2–3 [7]–[9]; ONI, *Submission 8*, 10–11.

271 *AGD Review of Secrecy Provisions* (n 149) 19.

272 See *AGD Review of Secrecy Provisions* (n 149).

273 AGD, *Submission 7*, 10 [42].

consolidation of the agency-specific secrecy offences in the *IS Act* (as noted above the Comprehensive Review did not consider the issues examined in this report).

- Persons who hold positions in intelligence agencies or who have privileged access to sensitive intelligence information should be held to a higher standard than other government officials.
- Robust secrecy offences provide foreign partner agencies with confidence that information they share with Australian intelligence agencies will be protected.[274]

4.208 It is difficult to agree that there are *significant* differences in the scope of the offences (either now or if the recommendations of this review are accepted). As discussed below, there are slight differences in who is covered by the offences (although this could be resolved with minor drafting adjustments) and the penalties are substantially the same in most cases. The main difference is which defences are available.

4.209 Comments about the particular position of trust held by intelligence officials and others with privileged access to sensitive information is discussed in **Chapter 6** where **Recommendation 10** proposes that a breach of trust by those who hold the highest security clearance should attract an additional penalty under Part 5.6. Australia's international obligations and comparable partner offences are discussed in **Chapter 3.**

4.210 The concerns that non-agency submitters raised about the deemed harm offence relating to intelligence agency information apply equally to the secrecy offences in the *IS Act*, *ASIO Act* and *ONI Act*. In particular, the concern that the Law Council and others raised on the breadth of the deemed harm offence relating to intelligence information also applies to the secrecy offences in the *IS Act, ASIO Act* and *ONI Act*. Specifically, information made or obtained by or on behalf of ASIS, ASIO, ASD, AGO, DIO and ONI in connection with or that relates to their functions captures an incredibly broad range of information. It does not necessarily follow that all information relating to the exercise of an intelligence agency's functions is prejudicial or remains prejudicial for an indefinite period of time. An added concern is the significant degree of overlap between the secrecy offences in the *IS Act*, *ASIO Act* and *ONI Act* and the deemed harm secrecy offence in s 122.1 of the *Criminal Code*.

Who is covered by the offences?

4.211 The specific secrecy offences relating to ASIS, ASIO, ASD, AGO, DIO and ONI apply not only to persons who are or have been a staff member or employee of these agencies; they also apply to a person who has entered into a contract, agreement or arrangement with each of these agencies.[275] Intelligence agency staff and contractors are covered by the definition of

274 See eg, ASIS, *Submission 10*, 6–9 [29]–[49]; ASIO, *Submission 6*, 5–6 [27]–[30]; ASD, *Submission 4*, 3–4 [5]–[9]; DIG, *Submission 5*, 2–3 [7]–[9]; ONI, *Submission 8*, 10–11.

275 *IS Act* (n 223) ss 39–40M; *ASIO Act* (n 244) ss 18–18B; *ONI Act* (n 243) ss 42, 44.

'Commonwealth officer' in s 121.1 of the Criminal Code. As discussed in **Chapter 1**, the concept of an 'agreement or arrangement' is probably not much broader (if at all) than the category 'otherwise engaged to perform work for the Commonwealth', which is included in s 122.1 and each offence for officials in Part 5.6.

4.212 Submissions and evidence from intelligence agencies indicated that they consider that, if a person signs a non-disclosure agreement or security briefing form, it would mean they have entered into an 'agreement or arrangement' with an intelligence agency. If correct this would bring them within the scope of the secrecy offences in the *IS Act*, *ASIO Act* and *ONI Act*.[276] As the *Criminal Code* offences already apply to all Commonwealth officials and contractors, as well as those who are' otherwise engaged to perform work' for the Commonwealth, it is difficult to see that there would be many situations where signing a non-disclosure agreement or briefing form would add to the class covered by the *Criminal Code*. But, if there are such situations, this could be remedied by a minor adjustment to the drafting of s 122.1.

4.213 In relation to ASIS, the secrecy offences in the *IS Act* also apply expressly to a person who is an agent of ASIS.[277] In the context of the *IS Act* and ASIS's functions, this is a reference to a person who acts covertly on behalf of ASIS to obtain foreign intelligence or undertake other ASIS functions outside Australia. I agree that it is appropriate for ASIS agents to be covered by any deemed harm offence relating to intelligence and security officials (although the circumstances in which it would actually be practical or in the public interest to prosecute a covert foreign agent for disclosing information would seem to be limited). Nevertheless, if the ASIS offences were to be replaced by the *Criminal Code*, care should be taken to ensure that the coverage of ASIS agents remains the same.

Penalties are substantially the same

4.214 A number of agencies made reference to differences in penalties between the deemed harm offence in Part 5.6 of the Criminal Code and the deemed harm offences in the *ASIO Act*, *IS Act* and *ONI Act*. There is a difference. However, in most cases involving intelligence agency staff, the maximum penalties will be the same or slightly higher in the *Criminal Code*.

4.215 The maximum penalty for the deemed harm offences in the *ASIO Act*, *IS Act* and *ONI Act* is 10 years imprisonment.[278] The maximum penalty for the deemed harm offence in s 122.1(1) and the harm offence in s 122.2(1) is 7 years imprisonment, but it increases to 10 years for the aggravated offence (s 122.3(1)). The aggravating factors include that the person holds a high-level security clearance (**Recommendation 10**) – something that will almost always be

276 See eg, Mr Stephen McGlynn, ASD, *Public hearing transcript,* 25 March 2024, 67; Ms Jeustelle Staver, ONI, *Public hearing transcript,* 26 March 2024, 145; ASIS, *Submission 10*, [14]–[15], [28].

277 *IS Act* (n 223) ss 39, 40C, 40D.

278 *IS Act* (n 223) ss 39–40D; *ASIO Act* (n 244) ss 18–18B; *ONI Act* (n 243) ss 42, 44.

the case for intelligence officials (though presumably not ASIS agents). The penalty for the 'dealing with' offence in s 122.1(2) is potentially *higher* in the *Criminal Code* – 5 rather than 3 years – because of the additional 2 years for the aggravated offence.

4.216 If there was real concern that some people currently covered by the offences in the *ASIO Act, IS Act* and *ONI Act* would only be subject to a 7-year penalty under s 122.2 because they do not hold a relevant security clearance, this could be dealt with by adding a new aggravating circumstance to cover that category of people.

Difference in defences

4.217 A number of agencies also referred to differences in the defences that are available for the deemed harm offences in the *ASIO Act*, *IS Act* and *ONI Act* as compared to deemed harm offences in Part 5.6 of the *Criminal Code*.

4.218 There are only 2 specific defences mentioned in the *ASIO Act*, *IS Act* and *ONI Act*. These are that information has already been communicated or made available to the public with the authority of the Commonwealth; or the person communicates the information to IGIS for the purpose of the IGIS performing a function or duty under the *IGIS Act*.[279] Although not couched as a 'defence' like the equivalent in s 122.5(1), there is an exception for communication authorised in the course of duties that is applicable to the *ASIO Act*, *IS Act* and *ONI Act* offences.

4.219 The defences in s 122.5(4) of the *Criminal Code* that operate because of other laws such as the *Public Interest Disclosure Act 2013* (Cth) (PID Act) would also apply to the *ASIO Act, IS Act* and *ONI Act* because of the operation of those other laws.

4.220 Some agencies were concerned that the defence for persons engaged in the business of reporting news could apply to intelligence officials (etc.) if the offences in the in the *Criminal Code* were relied on. However, this defence does not appear to be directly relevant to intelligence officials, it only applies to journalists and the staff of news media organisations. In the event a journalist was engaged under a contract or otherwise performing work for an intelligence agency for some reason they would fall within the definition of an official but would no longer have access to the defence as they would not be 'engaged in the business of reporting news, presenting current affairs or expressing editorial or other content in news media'. I agree that officials should not be able to rely on the journalist defence for

279 See eg, *IS Act* (n 223) ss 39(2), 39(3), 40C(2), 40C(2A), 40D(2), 40D(2A); *ONI Act* (n 243) s 42(2), 42(3), 44(3) and 44(4); *ASIO Act* (n 244) ss 18A(2), 18A(2A), 18B(2) and 18B(2A).

information they obtained in the course of their duties (see **Chapter 9**) but this does not create a practical difference between the *Criminal Code* and related secrecy offences.

4.221 The defence of obtaining or providing legal advice (s 122.5(5A)) is not available in the intelligence agency specific offences, nor is the defence of prior publication (s 122.5(8)), although both of these are relatively narrow in scope. In particular, the prior publication defence does not apply to information the person obtained in the course of their work as a Commonwealth official.[280] If it is the intention that these offences not be available to intelligence officials express provision could be made for this in the *Criminal Code*, though this may add complexity to the drafting.

4.222 If applied to intelligence officials, the application of the *Criminal Code* defence for reporting maladministration (s 122.5(4A)) might be read narrowly for intelligence agencies given that the 'appropriate agency' for reporting to is probably the agency itself, IGIS or the National Anti-Corruption Commission.

4.223 It is difficult to predict how a court would interpret the absence of a defence akin to s 122.5(5) of the *Criminal Code* which concerns providing information to courts or tribunals, but it is unlikely a court would readily interpret any offence as restricting the ability of a person to provide information to a court – although it may require procedures such as those in the *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth) to be followed when involved. That is, in so far as that defence pertains to disclosing or 'dealing with' information for the purpose of communicating it to a court or a tribunal, it may be that the defence does not go much further than the common law and a similar protection would, in effect, be available for the deemed harm offences under the *ASIO Act, IS Act* and *ONI Act* in any event.

4.224 In summary, I acknowledge that there are some differences in the defences that are available between the deemed harm offences in Part 5.6 of the *Criminal Code* and the deemed harm offences in the *ASIO Act*, *IS Act* and *ONI Act*. However, the differences in available defences are not sufficient to justify the significant overlap between the deemed harm offences in the *ASIO Act*, *IS Act* and *ONI Act* and the deemed harm offences in Part 5.6 of the *Criminal Code*. If the deemed harm offences in the *ASIO Act, IS Act* and *ONI Act* were to be repealed, some defences could be excluded for intelligence officials when the revised deemed harm secrecy offences in Part 5.6 are redrafted if that is considered appropriate.

---

280 Note that the prior publication defence in s 122.5(8) also includes a requirement that the person reasonably believed that, having regard to the nature and extent of the prior publication, further communication or dealing would not cause harm to Australia's interests or the security or defence of Australia. As discussed in Chapter 9, the 'lawyers' defence is also currently limited to advice connected to Part 5.6.

ASIO's vetting function

4.225 ASIO has recently been given a new security vetting function including to conduct security vetting assessments for Australia's highest level of security assessment (to be called Top Secret Positive Assurance (TSPA)). This means that ASIO holds (or will soon hold) a large amount of information about the individuals who hold these TSPA clearances, as well as the methodologies and sources used to undertaken the assessments. I accept ASIO's evidence that foreign intelligence agencies would be extremely keen to access this pool of information so they can identify things about individual clearance holders that may make then vulnerable to cultivation. Similarly, I accept that, if exact methods, techniques and sources used to make a vetting assessment were disclosed to a foreign adversary, they could use that information to try to enable an 'agent' to obtain a clearance and thus access to Australia's most sensitive information.

4.226 ASIO officers (or more likely a very limited subset of them) will have access to the TSPA vetting data and methodologies. This information will generally (and appropriately) not be available to anyone outside ASIO. The deemed harm offence in the *ASIO Act* should cover the disclosure of this sort of information so that ASIO staff and affiliates entrusted with this large amount of highly sensitive information are discouraged from (and punished for) disclosures, which are always, or almost always, going to result in likely significant harm.

4.227 Some people outside ASIO will have some knowledge of the TSPA vetting system. For example, individuals who have been through the process will know they have a clearance and what sort of information they were asked for. Security officers in government agencies will presumably have a list of officials in their agency with different security clearances, including TSPA clearances. I have considered whether this means that ASIO's TSPA vetting information should be included in the s 122.1 offence as well as the *ASIO Act* offence. I have concluded that it should not. Individuals should not be subject to a new criminal penalty for disclosing they have a clearance (although this may be poor security practice and might result in an administrative sanction). The same can be said for agency security staff who reveal a list of clearance holders – although, in that case, the conduct may well result in the type of harm that can be proved for the purpose of an offence under s 122.2 or s 122.4. Vetting information should not be covered by s 122.1, as it would be excessive and unnecessary and appropriate harm-based offences are already available.

Specific offences to protect the identity of intelligence officials and agents

4.228 The *IS Act* and the *ASIO Act* contain specific offences to protect the identities of ASIS and ASIO staff and agents. The requirement to protect the identities of these individuals for their own safety and to ensure they can carry out their covert human intelligence functions is well

established.[281] These offences have recently been amended by the *Comprehensive Review Act #3*. The result is that the offences for ASIO and ASIS are now quite different to each other. Retaining separate offences for ASIS and ASIO means that if a person is charged with an offence it will be immediately apparent that the offence is in relation to the relevant agency. However, both agencies advised me that they were satisfied that the new offences appropriately provided for the unique circumstances of each agency. As these are specific offences that do not substantively overlap with the *Criminal Code* offences, it is not necessary to analyse them further in this review.

4.229 In addition to specific offences relating to disclosure of ASIS and ASIO identities the *Comprehensive Review Act #3* introduced 'cover employment' provisions for ASIS, ASIO and ASD. These protect against liability for the use of 'cover employment' to protect an identity, rather than creating new offences. The Comprehensive Review expressly recommended against introducing secrecy offences in relation to the identity of ASD staff including because of the breadth of ASD's functions.[282]

Findings and recommendations on IS Act, ASIO Act and ONI Act

4.230 There is significant overlap between the general offences in the agency-specific Acts and the general deemed harm offence in the *Criminal Code*. Replacing the existing general deemed harm offences for intelligence agencies with s 122.1 would be consistent with the principle of consolidating offences to reduce the overall number of secrecy crimes. Some care in drafting would be required to ensure that all individuals presently covered by the offences (such as ASIS agents) would continue to be covered by the new offence and that new defences were not added without consideration of whether they were appropriate. The penalties are already very similar and could be adjusted by adding a new aggravating circumstance if necessary.

4.231 Most of the intelligence agencies strongly opposed moving their offences into the *Criminal Code* – for example, because they consider that the additional defences in the *Criminal Code* should not be available. While there are some additional defences, they are relatively narrow in scope. It may complicate the drafting in the *Criminal Code* for some defences not to be available for a group of people who would otherwise fall into the definition of 'a Commonwealth official or person otherwise engaged to perform work for a Commonwealth entity', but it could be done to the extent necessary.

281 *2019 Comprehensive Review* (n 267) 104–107 [35.70]–[35.84]

282 *2019 Comprehensive Review* (n 267) 107–109 [35.85]–[35.96], recommendation 142.

4.232 For the same reasons discussed in relation to **Recommendation 2**, excessively broad deemed harm offences cannot be described as necessary and proportionate. Therefore, if the deemed harm offences in agency-specific intelligence legislation are to be retained, they should be narrowed to the same extent described in **Recommendation 2**, with any other disclosures concerning those agencies being the subject of harm-based offences, particularly s 122.2. 'Dealing with' offences should similarly be adjusted to accord with **Recommendation 7** in **Chapter 6**.

4.233 ASIO staff and affiliates disclosing information about ASIO's new function of assessing and granting the highest level of security vetting clearances presents a particular risk, especially considering the volume of that information ASIO holds or will hold. This information should be covered in the *ASIO Act* for ASIO staff and affiliates. For other Commonwealth officials, disclosure of vetting information should not be covered by the deemed harm offence but should be covered by the harm-based offences in s 122.2.

4.234 ASIS and ASIO staff and agents undertake covert human intelligence collection activities that put them in positions of particular risk if their identities are disclosed. The specific offences relating to the identity of current and former ASIS and ASIO staff, affiliates and agents should be retained.

RECOMMENDATION 4: If separate general 'deemed harm' offences are to be retained in the *Intelligence Services Act 2001*, the *Australian Security Intelligence Organisation Act 1979* and the *Office of National Intelligence Act 2018*, 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.**
- **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 under Part IVA of that Act.**

DIO functions

4.235 As noted above, DIO falls within the scope of the current deemed harm offence in s 122.1, as it is covered by the second part of the definition of 'inherently harmful information' in s 121.1(1)(c) relating to information obtained or made by or on behalf of a domestic of foreign intelligence agency in connection with the agency's functions.

4.236 However, as also noted above, unlike the other 5 agencies in the definition of 'domestic intelligence agency' in s 121.1(1), which all have specified statutory functions, DIO is an

administrative part of the Department of Defence and does not have defined statutory functions. Instead, DIO operates in accordance with a 'mandate', which is an administrative document prepared by the Department of Defence. The mandate has been publicly available on the Department of Defence website since shortly after the 2019 Comprehensive Review Report recommended it be published.

4.237 An issue raised in the Issues Paper and considered in the review is whether it is consistent with the rule of law for DIO's functions to form part of a serious criminal offence given that DIO's functions are not set by the parliament or subject to parliamentary scrutiny though the disallowance process.[283]

DIO's 'mandate'

4.238 AGD stated that in its view the absence of legislated functions for DIO does not raise issues of concern in the application of the offences in Part 5.6.[284] AGD said this was because it is not necessary for an agency's functions to be set out in legislation for the prosecution to be able to adduce evidence to demonstrate that a defendant was reckless that information was obtained or made by or on behalf of a domestic or foreign intelligence agency.[285] This is true, although it will make proof of that fact more difficult and does not address the basic rule of law concern.

4.239 In response to discussion on this matter in the Issues Paper, DIO said it 'is a multifaceted issue, which touches on complex questions of constitutional law, including the delegation of legislative power, and the construct of particular statutory offences'.[286] At the public hearing, DIO did not accept the need for its functions to be set out in legislation and pointed to the fact that DIO's mandate is publicly available.[287] In response to further questioning, DIO stated:

> [W]e … agree with the Attorney-General Department's offering, that the absence of legislative functions does not raise issues of concern in the application of general secrecy offences. The utility and the agility in being able to work with the Inspector-General of Intelligence and Security, the Director-General of National Intelligence, and a process which is particularly robust in that the Secretary of the Department of Defence, the Chief of Defence Force, before it is taken to the Deputy Prime Minister in his role as the Minister for Defence before any change is made to the mandate, does illustrate that there is a very robust process in place for the DIO mandate at this point in time.[288]

283 *INSLM Issues Paper* (n 156) [1.16], [2.46], [2,66]–[2.88], 46, issue 18.
284 AGD, *Submission 7*, 12 [52].
285 AGD, *Submission 7*, 12 [53].
286 DIG, *Submission 5*, 7.
287 Mr Gavan Reynolds, DIG, *Public hearing transcript,* 25 March 2024, 69.
288 Lieutenant General Gavan Reynolds, DIG, *Public hearing transcript,* 25 March 2024, 70.

4.240 Concerns were raised that DIOs functions form part of the deemed harm offence when its functions are not set out in legislation by the joint academic submission and the Law Council of Australia. As put in the joint academic submission:

> '[b]ecause the 'functions' of DIO are determined by the Executive, and the only documentation of them may not always be publicly available, an important element of determining whether the information is 'inherently harmful' relies on policy setting that are entirely within the control of the government, and changes to it are not subject to any parliamentary oversight'.[289]

4.241 The joint academic submission described this as a rule of law concern similar to the reliance on the PSPF for the scope of the deemed harm offence relating to security classified information.

4.242 As an alternative to putting DIO's functions into legislation, the joint academic submission suggested that the requirement for DIO's mandate to be made public be enshrined in legislation and that relevant legislation be amended so that IGIS may brief PJCIS on the potential impact of any future changes in DIO's mandate on the ambit of the secrecy offences in Part 5.6.[290] I do not consider this sufficient.

4.243 The Law Council strongly opposed retaining DIO in the definition of 'domestic intelligence agency' in s 121.1 and argued that '[t]he rule of law requires that the intended scope and operation of offence provisions should be unambiguous and key terms should be defined' and '[i]t is not appropriate for the scope of serious indictable offences … to be dependent on administrative discretion'.[291] The Law Council recommended that DIO be removed from the definition of 'domestic intelligence agency' in s 121.1 of the *Criminal Code* so that DIO's functions fell outside the deemed harm offence in s 122.1.[292]

4.244 DIO noted that the Comprehensive Review Report did not recommend placing DIO on a statutory footing. The main reasoning was that DIO (like ONI) does not exercise invasive statutory powers like ASIO or have the immunities that ASIS, ASD and AGO have.[293] It seems that the Comprehensive Review Report did not consider the issue in the context of the Part 5.6 offences and the rule of law implications or the uncertainty that goes with having an offence that relies on a policy document to determine its scope.

4.245 There is also a question as to whether the DIO functions referred to in the *Criminal Code* are the functions as they were at the time the offence was created or if they are the functions as amended from time to time by the executive. This issue is the same as the one concerning

289 Joint Academic Submission, *Submission 13*, 10–11.
290 Joint Academic Submission, *Submission 13*, 11.
291 Law Council of Australia, *Submission 19*, 25 [66].
292 Law Council of Australia, *Submission 19*, 25, recommendation 5.
293 DIG, *Submission 5*, 7.

the PSPF that was discussed earlier in this chapter. This matter would be put beyond doubt by putting DIO's functions on a statutory footing.

Findings and recommendations on DIO's functions

4.246 Currently the *Criminal Code* and the *IS Act* both describe serious criminal offences by reference to DIO's functions. Those functions are not set in legislation; they are set by a policy document that the Department of Defence generates. That document can be changed at any time. It is not appropriate for the scope of a serious criminal offence to be changeable in this way.

4.247 I have no reason to doubt DIO's assertion that it needs to be an 'agile' organisation. I expect the other intelligence agencies also describe themselves as 'agile'. Statutory functions do not need to be narrowly drawn so long as they are clear. If necessary, some or all functions could be defined in regulations to make amendment easier.

4.248 Also, I have no reason to doubt that DIO engages with IGIS, the Department of Defence and relevant ministers on changes to its mandate. That is important, but it is not a substitute for the role of the parliament in setting the boundaries of crimes.

4.249 Parliamentary oversight and clarity in the operation of the exceptions for DIO in the *Freedom of Information Act 1982* (Cth) and the *Privacy Act 1988* (Cth) and the way DIO information is dealt with in the PID Act would also greatly benefit from the functions of DIO being set out in legislation or a disallowable legislative instrument.

RECOMMENDATION 5: The functions of the Defence Intelligence Organisation should be set out in legislation or in a disallowable legislative instrument.

4.250 If this recommendation is not accepted, I recommend that the *IS Act* be amended to repeal the secrecy offences in so far as they apply to DIO, as they are dependent on DIO's functions, and that the revised s 122.1 not include DIO. The disclosure of DIO information that is likely to harm security, defence or international relations would continue to be covered by s 122.2. The specific offences in the *Defence Act 1903* (Cth) and, where applicable, the *Defence Force Discipline Act 1982* (Cth) would also continue to apply.

Chapter 5: Serious harm-based offences

5.1 The offence in s 122.2(1) of the *Criminal Code* has many similarities to the offence in s 122.1, discussed in **Chapter 4**: both have a 7-year penalty (or 10 if aggravated) and both apply to current and former Commonwealth officers and others engaged to perform work for a Commonwealth entity. The main difference is that the offence in s 122.2(1) is harm-based. That is, to commit an offence under s 122.2(1), the communication of the information must be shown to cause or be likely to cause harm to one or more of a list of interests.

5.2 The communication offence in s 122.2(1) has a related 'dealing with' offence in s 122.2(2). The 'dealing with' offences are discussed in **Chapter 6**, as are other associated offences.

5.3 As discussed in **Chapter 1** and **Chapter 4**, previous reviews have recommended that secrecy offences be harm-based. Section 122.2 is consistent with this approach.

5.4 The types of harm that attract liability under s 122.2 are described by the defined term 'cause harm to Australia's interests'. This expression is defined in s 121.1 as follows:

> ***cause harm to Australia's interests*** means to:
>
> (a) interfere with or prejudice the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth; or
>
> (b) interfere with or prejudice the performance of functions of the Australian Federal Police under:
>
> (i) paragraph 8(1)(be) of the *Australian Federal Police Act 1979* (protective and custodial functions); or
>
> (ii) the *Proceeds of Crime Act 2002*; or
>
> (c) harm or prejudice Australia's international relations in relation to information that was communicated in confidence:
>
> (i) by, or on behalf of, the government of a foreign country, an authority of the government of a foreign country or an international organisation; and
>
> (ii) to the Government of the Commonwealth, to an authority of the Commonwealth, or to a person receiving the communication on behalf of the Commonwealth or an authority of the Commonwealth; or
>
> (f) harm or prejudice the health or safety of the Australian public or a section of the Australian public; or
>
> (g) harm or prejudice the security or defence of Australia.

5.5 Each part of this definition is discussed in this chapter. Because each of the parts of the definition begins with the phrase 'interfere or prejudice' or the phrase 'harm or prejudice', these thresholds are discussed first.

To prejudice, harm or interfere with

5.6 Each part of the definition of 'cause harm to Australia's interests' begins with 'interfere with or prejudice' or 'harm or prejudice'. The difference in terms used in different parts of the definition might in part be explained by the kinds of interests to which those verbs attach. However, the 'or' in these phrases appears to be disjunctive, and parliament has presumably intentionally used different words in different paragraphs. In other words, potentially, each of the terms 'interfere with', 'prejudice' and 'harm' has a different meaning.

Prejudice

5.7 The term 'prejudice' is not defined for Part 5.6 of the *Criminal Code*. It is defined for Part 5.2 of the *Criminal Code*. That definition makes clear that embarrassment alone is not sufficient to prejudice Australia's national security. It seems anomalous that the same clarification is not provided in Part 5.6. If the term 'prejudice' is retained in s 122.2, the *Criminal Code* should make clear that embarrassment alone is not sufficient to cause any of the harms described in Part 5.6 (but see comments below on international relations).

Harm

5.8 The word 'harm' is not defined in Part 5.6, but it is defined in the Dictionary to the *Criminal Code*:

> **harm** means physical harm or harm to a person's mental health, whether temporary or permanent. However, it does not include being subjected to any force or impact that is within the limits of what is acceptable as incidental to social interaction or to life in the community.

5.9 In accordance with s 4 of the *Criminal Code*:

> (1) Expressions used in the Code (or in a particular provision of the Code) that are defined in the Dictionary at the end of the Code have the meanings given to them in the Dictionary.
>
> (2) Definitions in the Code of expressions used in the Code apply to its construction except insofar as the context or subject matter otherwise indicates or requires.

5.10 The physical and mental health harm described in the Dictionary makes sense in the context of 'harm or prejudice the health or safety of the Australian public or a section of the Australian public', but it does not sit easily with other parts of the definition of 'cause harm to Australia's interests' such as 'harm to international relations' and 'harm to security or defence'. One explanation may be that the Dictionary definition appears to be directed to the meaning of 'harm' as a noun rather than as a verb. In any event, the presumption that the definition in the Dictionary applies is probably rebutted for the other parts of the definition of 'cause harm to Australia's interests'. This is a little awkward and is something that might be considered if the provision is redrafted in accordance with the recommendation made by this chapter, but it is not legally problematic.

5.11 The Human Rights Law Centre (HRLC) submitted that, due to the seriousness of the penalty, the threshold for the offence should be 'serious harm' and not just 'harm' and that this would also more closely align with the principles set out by the Australian Law Reform Commission (ALRC).[294] The Law Council of Australia made a similar point.[295] 'Serious harm' is defined in the Dictionary to the *Criminal Code*:

> ***serious harm*** means harm (including the cumulative effect of any harm):
> (a) that endangers, or is likely to endanger, a person's life; or
> (b) that is or is likely to be significant and longstanding.

5.12 It is unclear whether the definition of 'serious harm' picks up the definition of 'harm' above. The first part of this definition is clearly connected to 'harm' to people, but the second could be applied to other harms, such as harm to international relations.

5.13 It may be that the intention of the HRLC and the Law Council was not that the *Criminal Code* definition of 'serious harm' be used, but rather that the drafting of the provision convey that the harm required for a serious offence to be made out should be more than slight harm or mere interference and that it be in some way a material or significant harm.

Interfere

5.14 The Law Council of Australia considers that 'interference' is a much lower threshold than prejudice or harm.[296] Similarly, the Australian Human Rights Commission (AHRC) said that to 'interfere' with a law enforcement investigation is a low threshold that may criminalise 'innocuous conduct' and 'inhibit legitimate criticism of law enforcement officials who have acted inappropriately'.[297] The AHRC recommended that the term 'interfere' be removed from the definition of 'cause harm to Australia's interests'.[298]

5.15 The Law Council suggested replacing 'interfere' with 'impede' or 'seriously prejudice' and noted that the equivalent United Kingdom offence uses 'impede'.[299] The joint academic submission made a similar suggestion.[300]

---

294 Human Rights Law Centre, *Submission 14*, 11.
295 Law Council of Australia, *Submission 19,* 37 [128].
296 Law Council of Australia, *Submission 19*, 29–30, referring to *Gold Coast City Council v Satellite & Wireless Pty Ltd* (2014) FCR 412, [22]–[37].
297 Australian Human Rights Commission (AHRC), *Submission 17*, 11 [30].
298 AHRC, *Submission 17*, 12, recommendation 1.
299 Law Council of Australia, *Submission 19*, 29–31.
300 Joint Academic Submission, *Submission 13*, 14.

5.16 The Attorney-General's Department (AGD) was concerned that removing the definition of 'interference' may create new risks to Australian Federal Police (AFP) investigations:

> if interference is not covered, the AFP would have to wait for a criminal investigation to be actually prejudiced or harmed before being able to investigate the matter as a secrecy offence. This, in turn, would create risks to the Commonwealth that can be avoided if the AFP is able to intervene at an earlier stage.[301]

5.17 However, AFP's own policies indicate that it is unlikely to prioritise investigating or prosecuting an action that does not cause harm (see **Chapter 10**). Where applicable, the ancillary offences in Part 2.4 of the *Criminal Code* including attempt and incitement also apply.

5.18 Give that the term 'interfere' is currently used alongside either 'harm' or 'prejudice' in each element of the definition, it is likely that a court would interpret it as having a different, and lower, threshold than the other terms. Interference that is not material, such as minor delay or inconvenience, does not warrant the type of serious penalty imposed by s 122.2.[302]

Finding on threshold of harm

5.19 It is ultimately a matter of drafting to determine which terms are selected, but it would improve clarity to use a single term and not 2 disjunctive terms. It is my intention that the threshold for the types of harm covered by s 122.2 be one that requires material harm or the likelihood of such harm.

5.20 In the case of national security matters, where the potential for harm generally arises because of the damage that could be caused by a foreign actor in possession of the information, it should not be necessary (and indeed will probably not be possible) to prove that the foreign actor is actually in possession of the information. It is sufficient to show that the relevant harm is likely as a result of the conduct.

5.21 The role of the 'mosaic effect' in determining criminal culpability and harm has already been discussed in **Chapter 2**.

Prevention, detection, investigation etc. of criminal offences

5.22 The first part of the definition of 'cause harm to Australia's interests' applies to any interference or prejudice to the prevention, detection, investigation, prosecution or punishment of a criminal offence against any law of the Commonwealth. This is very broad.

---

301 Attorney-General's Department (AGD), *Submission 7*, 14.

302 Note that there are other offences for obstructing Commonwealth officials, including s 19.1 of the *Criminal Code Act 1995* (Cth).

There are a large number of agencies which have a role in the prevention (etc.) of offences against a very large number of Commonwealth laws. The provision is not limited to serious offences nor interference with police agencies.

5.23 The Law Council of Australia suggested that the offence should only apply to prejudice to *serious* offences:

> At the very least, it should be recognised that purported harm by unauthorised disclosure to law enforcement interests should only fall within a category of deemed harm secrecy offence where there is serious prejudice to detection and investigation of serious offences.
>
> In this regard, the Law Council considers that the application of paragraph 122.1(1)(a) to all Commonwealth offences – regardless of the severity of the offence –is unduly harsh. The Law Council considers it disproportionate that '(a)s a consequence, the maximum 7-year penalty (or 10 if aggravating circumstances exist) for disclosing information that is likely to cause interference or prejudice may be much harsher than the original offence'. As a minimum, it should only apply to the investigation or enforcement of 'serious Commonwealth offences' within the meaning of section 15GE of the *Crimes Act 1914* (Cth).[303]

5.24 AGD had a differing view, stating:

> interfering with or prejudicing a criminal investigation causes harm to the administration of justice and the rule of law, irrespective of the seriousness of the offence that is being investigated.[304]

5.25 Whether it would be practical to define and limit the offence by reference to 'serious offences' was tested at the public hearings. AFP did not express a view, deferring to the Attorney-General on this as a policy matter.[305] AGD was of the view that it would be very difficult to differentiate crime types and that sometimes the exact offence might not be evident at the start of an investigation, which may make it difficult to establish whether the prevention, detection or investigation of a crime was for a 'serious' crime. The Department also noted that different Acts have different thresholds for when a crime is 'serious'.[306]

---

303 Law Council of Australia, *Submission 19*, 30 [89]–[90].

304 AGD, *Submission 7*, 18.

305 Mr Stephen Nutt, Acting Assistant Commissioner, Australian Federal Police (AFP), *Public hearing transcript,* 25 March 2024, 101.

306 For example, 'serious offence' for certain search and other powers in Part IAA of the *Crimes Act 1914* (Cth) is an offence punishable by 2 years imprisonment. A 'relevant offence' for the *Surveillance Devices Act 2004* (Cth) includes an offence punishable by more than 3 years. The *Telecommunications (Interception and Access) Act 1979* (Cth) ('*TIA Act*') has a complex definition of serious offence in s 5D of that Act. Some provisions of the *Criminal Code* are tied to conviction for serious offences where the penalty is imprisonment for more than 7 years – e.g. Division 105A of the *Criminal Code*.

5.26 AGD also considered that a key issue was protection of law enforcement methodologies and capabilities,[307] which may in some cases be the same regardless of whether the crime being investigated is a 'serious' one. The Department of Home Affairs agreed that the capabilities used to investigate serious offences need to be protected.[308]

5.27 After further consideration and discussions with agencies, I agree that it is specific capabilities that require additional protections – that is, capabilities (and associated technology and methodologies) – that enable law enforcement agencies to exercise special powers. The parliament has already set thresholds for the types of offences that specific types of special capabilities can be used for, making it unnecessary to create a new definition of 'serious offences' for s 122.2 if the focus is shifted to protecting capabilities. Seeking to divide the offence between 'serious offences' and other offences may be arbitrary and also impractical for the reasons given by AGD.

5.28 During this review I also considered whether this part of s 122.2 should be redrafted to focus only on interference with the investigations (etc.) of a small number of 'law enforcement' agencies such as AFP, Australian Criminal Intelligence Commission as well as the National Anti-Corruption Commission. While initially attractive as a way to narrow the focus of the offence, I ultimately concluded that it is a somewhat arbitrary way to divide agencies. The parliament has given a broad range of agencies specific statutory powers to conduct searches, obtain information and exercise other special powers in the course of investigating (etc.) Commonwealth offences. It is the capability to exercise the special powers granted by parliament, rather than the agency which the parliament has granted to the power to, that seems a more logical divide.

Finding on law enforcement related disclosures

5.29 As discussed in **Chapter 4**, any intentional or reckless interference with the integrity of the criminal justice system or disclosures that would undermine law enforcement capabilities is serious and deserves some type of sanction. However, it does not follow that an offence that attracts a 7–10-year penalty is a necessary and proportionate response to every interference or prejudice to the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth.

5.30 Consistent with **Chapter 4**, I recommend a cascading approach to penalising disclosures that prejudice law enforcement related capabilities and other interferences with the criminal justice process. These should sit alongside existing specific offences for things such as attempting to pervert the course of justice and witness protection offences.

307 Ms Sarah Chidgey, AGD, *Public hearing transcript,* 26 March 2024, 152.
308 Mr Nathan Smyth, Department of Home Affairs, *Public hearing transcript,* 25 March 2024, 83.

5.31 In accordance with **Recommendation 3**, the deemed harm offence in s 122.1 should apply to the specialised technologies, capabilities and methods that support the extraordinary electronic surveillance powers that parliament has granted a small number of agencies.

5.32 The harm-based offence in s 122.2 should impose the higher penalty (7 years imprisonment or 10 years imprisonment for an aggravated offence) on disclosures which undermine the utility of technologies, capabilities and methodologies connected to special statutory powers granted to investigate and prosecute crimes. Unlike the narrow class of electronic surveillance capabilities of be covered in s 122.1, it is not necessarily the case that every disclosure about the broader range of capabilities in s 122.2 will always or almost always cause harm. Whether harm is caused will depend on the specific facts of what was disclosed and how it impacts, or does not impact, capabilities. Some of these capabilities are overt and a disclosure about how they are exercised will not cause harm. This makes it important that the offence in s 122.2 requires proof of harm or likely harm.

5.33 Some examples of the operational capabilities and methods intended to be covered by s 122.2 include those relating to the exercise of:

- the stop, search and seize powers under Division 3A of the *Crimes Act 1914* (Cth) in relation to terrorist acts and terrorism offences
- search warrants under the *Crimes Act*, *Customs Act 1901* (Cth) and *Australian Crime Commission Act 2002* (Cth), including technical capabilities such as forensic tools used to examine electronic devices or files seized under a search warrant [309]
- monitoring warrants under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth)[310]
- powers to require the production of information, including under financial and taxation laws[311]
- telecommunications data access authorisations.[312]

5.34 Unlike the existing s 122.2, the proposed new offence will apply to the *capability* and it will not be necessary to show that a particular investigation (etc.) was prejudiced. For example, if a new capability had been developed or purchased and an unauthorised disclosure meant

309 *Crimes Act* (n 306) ss 3E-3F; *Customs Act 1901* (Cth) s 198; *Australian Crime Commission Act 2002* (Cth) s 22.

310 *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 159.

311 Some examples include the *Australian Securities and Investments Commission Act 2001* (Cth) ss 19, 30, 30A, 30B, 31, 32A and 33; *Tax Administration Act 1953* (Cth) s 353-10.

312 *TIA Act* (n 306) pt 4.1.

that capability would not be able to perform as intended then this may be sufficient to establish the necessary harm even if the capability had never been used.

5.35 Because the offence will apply to any Commonwealth official or other person otherwise engaged to perform work for a Commonwealth entity (see **Chapter 1**), it will have wider application than most current agency-specific offences. Whether all of the existing specific secrecy offences that relate to these specific powers remain necessary in light of the amendments to Part 5.6 recommended by this review and the new general secrecy offence is something that could be considered as part of the ongoing implementation of the AGD *Review of Secrecy Provisions*.[313]

5.36 As discussed in **Chapter 7** and in accordance with **Recommendation 11** the proposed new general offence for Commonwealth officials should apply to disclosures that prejudice the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth. There may be some overlap between the proposed general offence and the new ss 122.1 and 122.2 but the intent is that the general offence apply to disclosures that prejudice specific investigations (etc) while ss 122.1 and 122.2 apply to disclosures which would undermine the utility of capabilities used to investigate many offences.

AFP protective and custodial functions and proceeds of crime matters

5.37 Paragraph (b) of the definition of 'cause harm to Australia's interests' covers AFP's protective and custodial functions as well AFP's functions under the *Proceeds of Crime Act 2002* (Cth) (*POC Act*).

Protective and custodial functions

5.38 In accordance with s 8(1)(be) of the *Australian Federal Police Act 1979* (Cth) (*AFP Act*):

> [It is an AFP function to] perform such protective and custodial functions as the Minister directs by notice in writing in the Gazette, being functions that relate to a person, matter or thing with respect to which the Parliament has legislative power;

5.39 Early in the process of this review AFP provided a copy of a notice signed by the relevant Minister setting out what was described as protective and custodial functions. AFP advised that the document had not been published on the Federal Register of Legislation.[314] During

313 AGD, *Review of Secrecy Provisions* (Final Report, 21 November 2023).

314 Since October 2012 the Gazette has been published in an electronic and searchable format on the Federal Register of Legislation. The Government Gazette contains notices regarding legislation and other notices required to be published under Commonwealth law.

the review AFP advised that it was seeking legal advice and was taking steps to ensure that the publication requirements of s 8(1)(be) of the *AFP Act* were met.

5.40 In addition to satisfying the publication requirements of s 8(1)(be) of the *AFP Act*, it is important that the scope of the protective and custodial functions is set out clearly in a public instrument so that the boundaries of the offence in s 122.2 are 'knowable' – a key rule of law requirement as discussed in **Chapter 4**.

5.41 Protective and custodial functions are a core part of AFP's role, and the proper performance of those functions is important to public safety and the safety of individuals who are under specific protection arrangements.

Proceeds of crime

5.42 The AFP described their functions under the *POC Act* as:

> depriving persons of the proceeds, benefits and instruments derived from offences against the laws of the Commonwealth, to punish and deter persons from breaching laws of the Commonwealth, and to prevent the reinvestment of proceeds, instruments and benefits of offending in further criminal activities, amongst others.[315]

5.43 The proceeds of crime functions are civil and administrative measures, not criminal.

5.44 The ALRC report *Secrecy Laws and Open Government in Australia* (ALRC 2009 Secrecy Laws Report) considered whether the proceeds of crime functions should be included in a general secrecy offence and concluded that it should not:

> The general criminal offence should not extend to unauthorised disclosures of information that would prejudice the enforcement of laws relating to the confiscation of the proceeds of crime, or the protection of the public revenue. Taxation legislation and proceeds of crime legislation already contain specific secrecy offences targeting Commonwealth information in those contexts.[316]

5.45 In its submission to the AGD Review of Secrecy Provisions, the Law Council of Australia echoed this position, saying it was excessive to impose criminal sanctions in a general secrecy offence on disclosures that threaten civil or administrative processes and that, to the extent that an offence is necessary, it should be a specific offence.[317]

---

315 AFP, *Submission 18*, 9.

316 Australian Law Reform Commission (ALRC), *Secrecy Laws and Open Government in Australia* (Report No 112, December 2009) 157 [5.63] (ALRC 2009 Secrecy Laws Report).

317 Law Council of Australia, Submission (ID No 44186415) to AGD *Review of Secrecy* Provisions (22 May 2023) 20.

5.46 In discussions held with AFP during this review, AFP advised that proceeds of crime actions have become an increasingly important tool in combating serious and organised crime, including in situations where the alleged 'principals' are outside Australia and in a jurisdiction where extradition is not a viable option. AFP said:

> Effective proceeds of crime action appropriately deprives offenders of the benefits of criminal activity, removes the instruments used to facilitate offending, and prevents the reinvestment of illicit proceeds into further criminal activities.[318]

5.47 The unauthorised release of information about *POC Act* investigations or proceedings creates a real risk that relevant assets would be moved, concealed or dissipated, frustrating the principal objects of the *POC Act*. AFP said that, although there are specific offences in the *POC Act*, they have limited scope and only prohibit the recipient of an order requiring the production of documents/information from disclosing the existence, and nature, of the particular order.

5.48 Although proceeds of crime matters are themselves not criminal proceedings, they are tied closely to the enforcement of the criminal law. As AGD said, 'the very close link between criminal investigations and proceeds of crime matters is a reason for treating these similarly in the application of secrecy offences'.[319] In the context of the advice from AFP and AGD, it seems reasonable that proceeds of crime operations and methodology should receive similar treatment to other special methods provided for in enactments to combat serious criminal offending.

Finding on protective, custodial and proceeds of crime function

5.49 Subject to the AFP protective and custodial functions being properly published, it is reasonable for them to continue to be included in the scope of the offences in s 122.2.

5.50 Similarly, AFP functions under the *POC Act* should be retained in the scope of s 122.2. My intention in this regard is that the kinds of harmful disclosures that would be covered in the offence would be those that are likely to materially affect AFP's ability to utilise the special powers available under that Act.

International relations

5.51 Paragraph (c) of the definition of 'cause harm to Australia's interests' relates to harm or prejudice arising from information communicated to the Commonwealth by a foreign country, government or international organisation. It requires proof that the original

318 Email from AFP to INSLM, 9 May 2024.
319 AGD, *Submission 7*, 14.

communication to the Commonwealth was in confidence and that the unauthorised disclosure caused or would likely cause harm or prejudice to 'international relations'.

5.52 The requirement that harm or likely harm result from the disclosure means that information which was originally communicated in confidence but which is no longer confidential because no harm would result from its disclosure is not penalised. A similar result is achieved in the *Archives Act 1983* (Cth) through a different mechanism – that Act allows disclosure of information that was originally passed in confidence to be released if it is no longer reasonable to maintain the confidentiality.[320]

5.53 The term 'international relations' is currently defined to have the same meaning as the defintion in the *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth) (*NSI Act*),[321] which provides:

> ***international relations*** means political, military and economic relations with foreign governments and international organisations.[322]

5.54 Some examples of the types of harm this provision was intended to cover are provided in the Revised Explanatory Memorandum to the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 (EFI Bill). They include:

- the lessening or cessation of military or intelligence cooperation
- damage to Australia's negotiating position in respect of a treaty or agreement, or within an international organisation such as the United Nations or an organ thereof
- a reduction in the quality or quantity of information provided by a foreign government or international organisation
- loss of confidence or trust in the Australian Government by an overseas government or international organisation

---

320 *Archives Act 1983* (Cth) s 33. Under this provision in order for a Commonwealth entity to refuse to release the information it is necessary to establish that the foreign entity has advised the Commonwealth that the information is still confidential and also to establish that the confidentiality is reasonable to maintain.

321 Grant Donaldson, INSLM (former), *Review into the operation and effectiveness of the National Security Information (Criminal and Civil Proceedings) Act 2004* (Report, 30 October 2023) 110, recommendation 2 ('*INSLM NSI Act Report*') recommended that the definition of 'international relations' be changed from 'political, military and economic relations with foreign governments and international organisations' to 'diplomatic and military relations with foreign governments and international organisations'.

322 *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth) s 10. The *INSLM NSI Act Report* (n 321) recommended this definition be amended to 'diplomatic and military relations' where the term 'diplomatic' was considered a more 'limited and concise term' than 'political' and the term 'economic relations' was removed as it was considered 'too broad and imprecise': see 111 [406].

- a detrimental impact on the ability of the Australian Government to maintain good working relations with a foreign government or international organisation
- intangible damage to Australia's reputation or relationships between the Australian Government and a foreign government or international organisation, or between officials, having the effect of diminishing the capacity of the Australian Government to function in the global political, military and economic environment.[323]

5.55 In its submission to this review, AHRC said that the definition of 'causes harm to Australia's interests' was overly broad and may capture the disclosure of information that is not sufficiently harmful to warrant criminalisation.[324] AHRC recommended that the definitions be amended to make them clearer and to ensure that only a narrow range of offences was covered.[325]

5.56 Submissions to the Parliamentary Joint Committee on Intelligence and Security review of the EFI Bill noted that the definition of 'international relations' could capture confidential information that does not necessarily cause harm to Australia's international relationships,[326] such as reporting on international trade.[327] The Law Council of Australia's submission to the INSLM review of *NSI Act* said that the definition of 'international relations' in the *NSI Act* was too broad, and highlighted the conclusions of the AHRC that:

> prohibiting a disclosure that merely embarrasses the Australian Government, without threatening real damage to international relations, is unlikely to be a proportionate restriction on Article 19 of the International Covenant on Civil and Political Rights …[328]

5.57 This concern about *mere* embarrassment can be resolved by ensuring that prejudice does not include mere embarrassment as suggested earlier in this chapter. However, in the context of diplomatic relations, embarrassment can sometimes cause actual harm, including a reduction in cooperation or provision of information to Australia. Such a result is not 'mere' embarrassment; it would be actual harm, and that should remain covered by the offences. Proof would be required that the harm had occurred or was likely to occur.

---

323 Revised Explanatory Memorandum, National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017, 259 [1245].

324 AHRC, *Submission 17*, 11 [29].

325 AHRC, *Submission 17*, 12, recommendation 1.

326 Parliamentary Joint Committee on Intelligence and Security (PJCIS), Parliament of Australia, *Advisory Report on the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (Report, June 2018) 121-122 [4.79]–[4.81] ('*PJCIS EFI Bill Report*').

327 *PJCIS EFI Bill Report* (n 326) 122 [4.80].

328 Law Council of Australia, Submission No 11 to INSLM, *Review into the operation and effectiveness of the National Security Information (Criminal and Civil Proceedings) Act 2004* (26 June 2023) 9 [19].

5.58 There was also concern that including 'economic relations' makes the definition too broad. In this regard, the AHRC said the definition of 'international relations' is broad, and it is unclear if the reach of the 'economic' aspect of the definition would criminalise unauthorised disclosures about corporations.[329] Similarly, the Law Council of Australia said that the inclusion of 'economic relations' would risk the secrecy offence attaching to a variety of commercial transactions remote from damaging international relations.[330]

5.59 The UK Law Commission recommended against expanding the equivalent UK offence protecting national security to include economic information.[331]

5.60 It is doubtful whether damage solely to the economic position of an Australian company, rather than the economic wellbeing of the nation, would fall within the existing definition, given that it refers to 'economic relations with foreign governments and international organisations'. But the term 'economic relations' is broad and, rather than specify 'economic' and 'political' relations separately, it may be sufficient to say 'diplomatic' relations – a category that is intended to be broad enough to encompass damage to the full spectrum of the relationship between Australia as a body politic and other countries.[332]

5.61 The current definition of 'international relations' does not expressly pick up bilateral and multilateral law enforcement and intelligence cooperation arrangements. By these categories I mean arrangements such as the Five Eyes intelligence sharing arrangement, AUKUS, the INTERPOL arrangement and AUSTRAC's international financial intelligence sharing agreements. It may be that these are captured by the term 'political' in the current definition (or alternatively 'diplomatic' relations). However, the definition should be amended to ensure that there is no doubt that harm to these important international information sharing arrangements are covered by the revised offence in s 122.2.

Findings on international relations

5.62 The offence in s 122.2 should continue to cover harm to international relations. But the definition of 'international relations' and the way the harm is described should be amended.

5.63 The definition of 'international relations' should cover diplomatic and military relations with foreign governments and international organisations, as well as bilateral and multilateral law enforcement and intelligence cooperation arrangements. It is intended that this includes disclosing information communicated in confidence by a foreign government, an authority

329 AHRC, *Submission 17*, 11 [31].

330 Law Council of Australia, *Submission 19*, 32 [98].

331 Law Commission (UK), *Protection of Official Data* (Report No 395, 1 September 2020) 118 [5.205].

332 The Law Council of Australia supported this type of construction of a definition of 'international relations': see Law Council of Australia, *Submission 19*, 32 [99]. Military cooperation may need to be in its own category as military matters are often distinguished from diplomatic maters, particularly in times of armed conflict.

or an international organisation and which remains confidential for one or more of these purposes.

5.64 As discussed a little later in this chapter, harm to 'security' and 'defence' should also be separately referred to and defined.

Public health or safety

5.65 This element of the definition requires evidence that the unauthorised disclosure of information caused or would be likely to cause harm or prejudice to the health or safety of the Australian public or a section of the Australian public. It does not require the harm to be 'serious harm'.

5.66 The Revised Explanatory Memorandum to the EFI Bill said:

> causing harm to Australia's interest includes harming or prejudicing the health or safety of the Australian public or a section of the Australian public. The unauthorised communication of, or dealing in, official information that threatens public safety, or that threaten public health, are serious matters warranting criminal liability.[333]

5.67 AGD noted that the provision did not protect against disclosures that cause harm to the health and safety of an *individual* but 'applied a higher threshold of harm' to disclosures that cause harm to the health and safety of the Australian public or a section of the Australian public.[334]

5.68 It is difficult to identify many circumstances where the release of government information would actually harm or prejudice the health or safety of the Australian public or a section of the Australian public. This review did not specifically request examples of where this may occur, and none were identified in the Revised Explanatory Memorandum for the EFI Bill. However, the ALRC 2009 Secrecy Laws Report provided one example:

> The ALRC has concluded that unauthorised disclosures of information that are likely to prejudice the protection of public health – for example, the location of national supplies of a vaccine being stockpiled in a secure location in case of national emergency – would also prejudice the protection of public safety.[335]

5.69 The Law Council of Australia considered that this element of the definition was unjustifiably vague and could be applied to a 'vast range of situations where there is negligible harm'. The

333 Revised Explanatory Memorandum, National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2018 (Cth) 259 [1247].

334 AGD, *Submission 7*, 15 [68].

335 ALRC 2009 Secrecy Laws Report (n 316) [5.76]

Law Council recommended that the definition be amended to restrict the definition to 'serious harm' to the Australian public or sections of the Australian public.[336]

5.70 AGD said that it was not necessary for the conduct to be tied to serious harm:

> The harms-based approach does not require that an offence be limited to serious harm. Different degrees of harm may be covered by one offence and sentencing courts will apply different penalties that reflect the relative seriousness of the conduct within the maximum penalty that applies to the offence. Consistent with Principle 10 of the Secrecy Review, secrecy offences should have maximum penalties that reflect the potential seriousness of the conduct at its highest.[337]

Finding on public health or safety

5.71 It is apparent that the expression 'health or safety of the Australian public or a section of the Australian public' is not intended to be about harm to specific individuals. Rather, it is intended to cover matters that are more widespread and threaten public safety or public health more generally, although it would seem rare that the disclosure of government information would have this result. On this basis, it is not necessary to raise the threshold to 'serious harm', as widespread harms to public safety are by their nature serious matters, and these matters should remain within the offence in s 122.2.

Security or defence of Australia

5.72 Paragraph (g) of the definition of 'cause harm to Australia's interests' concerns harm or prejudice to the 'security or defence of Australia'. The expression 'security or defence of Australia' is defined in s 121.1 as follows:

> ***security or defence of Australia*** includes the operations, capabilities or technologies of, or methods or sources used by, domestic intelligence agencies or foreign intelligence agencies.

5.73 The Alliance for Journalists' Freedom (AJF) said the definition of 'cause harm to Australia's interests' in this respect was too broad and overly complex. In particular, AJF said that it 'could include information about an agency's budget, staffing arrangements, or training, or information that reveals corrupt, abusive, or unethical behaviour, the disclosure of which could cause no actual harm'.[338]

5.74 The joint academic group made a similar comment that the 'security and defence' part of the definition risked criminalising the disclosure of 'non-operational details that nonetheless

---

336 Law Council of Australia, *Submission 19*, 33 [102].
337 AGD, *Submission 7*, 15 [69].
338 Alliance for Journalists' Freedom (AJF), *Submission 11*, [5.6].

reveal corrupt, abusive or unethical behaviour'. While they considered that the journalism defence may be available if a prosecution were pursued in relation to a disclosure by a journalist, it was their view that the breadth and uncertainty of the definition contributed to the 'chilling effect'.[339]

5.75 AJF also suggested that it was inappropriate to give the same treatment to foreign and domestic intelligence agencies.[340] Conversely, many National Intelligence Community agencies spoke about the importance of international partnerships and intelligence sharing relationships, and this is discussed further in **Chapters 3** and **4**. It is also addressed in the finding above that those types of relationships should be clearly covered by s 122.2 as well as by **Recommendation 2**.

5.76 The current definition of 'security or defence of Australia' is unacceptably vague, particularly noting that the definition is not exhaustive. It is also unnecessary, as the specific matters highlighted in the definition are already covered by **Recommendation 2**. This does not mean that things that are actually harmful to security or defence should not be covered by s 122.2, but better definitions are needed.

5.77 The *Australian Security Intelligence Organisation Act 1979* (Cth) (*ASIO Act*) contains the following definition of 'security':

> ***security*** means:
>
> (a) the protection of, and of the people of, the Commonwealth and the several States and Territories from:
>
> (i) espionage;
>
> (ii) sabotage;
>
> (iii) politically motivated violence;
>
> (iv) promotion of communal violence;
>
> (v) attacks on Australia's defence system; or
>
> (vi) acts of foreign interference;
>
> whether directed from, or committed within, Australia or not; and
>
> (aa) the protection of Australia's territorial and border integrity from serious threats; and
>
> (b) the carrying out of Australia's responsibilities to any foreign country in relation to a matter mentioned in any of the subparagraphs of paragraph (a) or the matter mentioned in paragraph (aa).[341]

5.78 Many of the terms in the definition are further defined in the *ASIO Act*. The definition, particularly part (b), is broad.

---

339 Joint Academic Submission, *Submission 13*, 14.

340 AJF, *Submission 11*, [5.7].

341 *Australian Security Intelligence Organisation Act 1979* (Cth) s 4.

5.79 That said, this definition of 'security' is picked up by the *NSI Act* and other Acts. It is a widely accepted and used definition of 'security'. It has been the subject of judicial consideration, and it would be defensible to adopt it for the Part 5.6 *Criminal Code* offences. The definition of 'national security' in Part 5.2 is not an appropriate alternative, including because it refers to 'defence' and also refers to Australia's 'political, military or economic relations with another country or other countries' (s 90.4).

5.80 The definition of 'defence' was recently considered by former INSLM, Mr Grant Donaldson SC, in his review of the *NSI Act*. Mr Donaldson SC adapted the definition of 'defence' from the UK *Official Secrets Act 1989*[342] and recommend 'defence' in the *NSI Act* be amended to provide that:

> *Defence* means:
>
> (a) the organisation, operations, state of readiness and training of the Australian Defence Force;
>
> (b) the weapons and other equipment of the Australian Defence Force;
>
> (c) research into, development, production and operation of weapons and other equipment of the Australian Defence Force;
>
> (d) defence strategy, military planning and military intelligence.[343]

5.81 This definition would be a good basis for developing a definition of 'defence' that is suitable for Part 5.6 of the *Criminal Code*. The alternative would be to leave the term 'defence' undefined and leave it to the courts to determine what it means. But a definition would be preferable because it would provide clarity on the scope of the offence.

Finding on security or defence of Australia

5.82 The current definition of the phrase 'security or defence of Australia' in s 121.1 is unclear and unnecessary and should be repealed.

5.83 Prejudice to the security or defence should remain covered by the offence in s 122.2 but not in the way it is currently defined. Instead, new definitions should be inserted, with 'security' being linked to the definition of 'security' in the *ASIO Act*. Also, a definition of 'defence' should be inserted based on the definition that Mr Donaldson SC recommended in his review of the *NSI Act*.

342 *Official Secrets Act 1989* (UK) s 2(4).

343 *INSLM NSI Act Report* (n 321) 110, recommendation 2.

Recommendation

RECOMMENDATION 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.**

5.84 Dealing with offences are discussed in **Chapter 6.** The same types of harm described in **Recommendation 6** should be applied to the dealing with offence for officials in s 122.2(2).

5.85 It would be preferable for one term to be used to describe the harm rather than using multiple verbs (such as 'prejudice or harm'), which is the current approach. A material level of harm should be required. While it is ultimately a matter for drafting, either 'prejudice' or 'harm' should be used rather than 'interfere with', the lower threshold for which does not justify the imposition of a serious offence.

5.86 'Security' should be defined as it is in the *ASIO Act.*

5.87 'Defence' should be defined in a way that incorporates matters directly connected to the defence of Australia, such as those described in recommendation 2.3 of the INSLM *Review into the operation and effectiveness of the National Security Information (Criminal and Civil Proceedings) Act 2004* report.[344]

5.88 'International relations' should cover the diplomatic and military relations with foreign governments and international organisations as well as bilateral and multilateral law enforcement and intelligence cooperation arrangements.

5.89 As discussed in **Chapter 4** in relation to **Recommendation 3**, the offences relating to law enforcement methodologies and capabilities should be cascading. The offence in s 122.2 is intended to impose a higher penalty on disclosures that could compromise powers exercised under warrants and authorisations granted to support the investigation of crime by any agency. This includes capabilities connected to statutory powers to access information or to search people, places or things. Parliament has granted these to a wide range of agencies in order to investigate a wide range of crimes. It is reasonable to expect that evidence of harm

344 *INSLM NSI Act Report* (n 321) recommendation 2.3.

can be established in order to justify a 7–10-year penalty for undermining this type of capability. Though some of these capabilities are sensitive, they are not in the same category of sensitivity as the extraordinary covert electronic surveillance powers to be covered by the deemed harm offence in s 122.1 (see **Recommendation 3**).

5.90 The recommendation to retain AFP protective and custodial functions in this offence is contingent on those functions being described in a publicly available legislative instrument (as appears to be required by s 8A of the *AFP Act*.)

5.91 Reference to 'harm to the health or safety of the Australian public or a section of the public' is the same as in the current s 122.2.

Chapter 6: Related offences

6.1 In addition to the communication offences in ss 122.1(1) and 122.2(1) of the *Criminal Code*, which are discussed in **Chapter 4** and **Chapter 5** respectively, Part 5.6 of the *Criminal Code* also contains related offences concerning 'dealing with' information, proper places of custody for information and failure to comply with lawful directions. There are also aggravated offences for ss 122.1 and 122.2. Each of these is discussed in this chapter.

6.2 For non-officials the disclosure offence in s 122(4A)(1) discussed in **Chapter 8** also has an associated 'dealing with' offence. The 'dealing with' part of that offence is discussed in this chapter.

'Dealing with' offences

6.3 The 'dealing with' offences are in a sense preparatory offences. They apply before a communication has occurred. However, the 'dealing with' offences in Part 5.6 are unusual preparatory offences because they do not require evidence of an intention to communicate information or even recklessness to a communication occurring.

6.4 Section 122.1(2) makes it an offence for a person who is or was a Commonwealth officer (or otherwise engaged to perform work for a Commonwealth entity) to 'deal with' (other than by communicating) 'inherently harmful information' made or obtained in the course of their work for the Commonwealth or a Commonwealth entity. Similarly, s 122.2(2) makes it an offence to 'deal with' information (other than by communicating) if the dealing 'causes harm to Australia's interests' or is likely to 'cause harm to Australia's interests'. As discussed in **Chapters 4** and **5**, the expressions 'inherently harmful information' and 'cause harm to Australia's interests' are defined terms that presently have very broad meanings. This chapter proceeds on the assumption that those definitions will be amended in accordance with **Recommendations 1–3** and **5–6**.

The definition of 'deal'

6.5 The definition of 'deal' for the purposes of the offences in Part 5.6 is provided by s 90.1(1) of the *Criminal Code:*

> A person ***deals*** with information or an article if the person does any of the following in relation to the information or article:
>
> a) receives or obtains it;
> b) collects it;
> c) possesses it;
> d) makes a record of it;
> e) copies it;

f) alters it;
g) conceals it;
h) communicates it;
i) publishes it;
j) makes it available.

6.6 Rather confusingly, 'communicating' is expressly excluded from each of the 'dealing with' offences and yet the definition of 'deals' expressly includes 'communicating'. 'Communicate' is defined in Part 5.6 (but not Part 5.2) as including 'publish' and 'make available'.[345]

6.7 Section 90.1(2) extends the meaning of 'deal' by providing that 'dealing with' information includes dealing with all or part of the information and dealing only with the substance, effect or description of the information or article.[346] The latter part of this extension gives the term an extremely wide meaning, particularly when combined with the definition of information:

> ***information*** means information of any kind, whether true or false and whether in a material form or not and includes an opinion and a report of a conversation.[347]

6.8 Most of the elements of 'deal' are not further defined in s 90.1(1) so have their ordinary meaning; however, a definition of 'make available' is provided in s 90(1):

> ***make available*** information or an article includes:
> a) place information somewhere it can be accessed by another person; and
> b) give it to an intermediary to give to another intended recipient; and
> c) describe how to obtain access to it, or describe methods that are likely facilitate access to it (for example, set out the name of a website, and IP address, a URL, a password or the name of a newsgroup).

6.9 This means that 'make available' in the definition of 'deal' for the 'dealing with' offences has the extended meaning given in s 90(1) of Part 5.2 of the *Criminal Code*. However, the term 'make available' is separately used in the definition of 'communicate' in s 121.1 in Part 5.6 of the *Criminal Code*. That definition of 'communicate' applies to both the 'communication' offences and to the exclusion of 'communicating' from the 'dealing with' offences and it does not incorporate the extended definition of 'make available'. This is because the definition of 'make available' in Part 5.2 only applies to the terms defined in Part 5.2 and those where Part 5.6 expressly points to a definition in Part 5.2. It is unclear whether this is intentional or not.

6.10 The 'dealing with' offences raise similar issues with breadth, uncertainty and the rule of law to those discussed in **Chapter 4** and **Chapter 5**. There are also questions about the necessity

345 *Criminal Code Act 1995* (Cth) s 121.1(2) ('*Criminal Code*').
346 *Criminal Code* (n 345) s 90.1(2).
347 *Criminal Code* (n 345) s 90.1(1).

and proportionality of 'dealing with' offences, particularly for non-officials. Many submissions to this review have raised the question as to whether the current definition of 'deal' is appropriate for an offence of this type. Of particular concern to submitters is that to 'deal' with information includes to merely *receive* information. These issues are discussed in this chapter but before turning to them it is useful to note similar offences in other Acts and to understand the applicable fault (mental) element.

'Dealing with' offences in related Acts

6.11 The *Intelligence Services Act 2001* (Cth) (*IS Act*) makes it an offence for staff members and certain others to deal with the records of Australian Secret Intelligence Service (ASIS), Australian Signals Directorate or the Australian Geospatial-Intelligence Organisation.[348] The drafting of this offence provides a shorter list of what constitutes 'dealing' but then ends with the catch-all 'dealing with a record in any other manner'. It is not clear if a court would read this phrase as being intending to cover only dealings in the same class as the earlier items or if it would be read more broadly. The relevant part of the dealing with offence provides

> 1) A person commits an offence if:
>
> a) the person engages in any of the following conduct (the relevant conduct):
>
> (i) copying a record;
>
> (ii) transcribing a record;
>
> (iii) retaining a record;
>
> (iv) removing a record;
>
> (v) dealing with a record in any other manner.[349]

6.12 There is a separate offence of making a record of any information or matter that came to the knowledge of the person in the course of their work for the intelligence agency.[350]

6.13 The same offences are also in the *Australian Security Intelligence Organisation Act 1979* (Cth) (*ASIO Act*)[351] and the *Office of National Intelligence Act 2018* (Cth) (*ONI Act*).[352]

---

348 *Intelligence Services Act 2001* (Cth) ('*IS Act*') ss 40C, 40D. The offences apply to people who obtained the information by reasons of being or having been 'staff members' (as defined), agents of the Australian Secret Intelligence Service (ASIS), a person who have a contract, agreement or arrangement with the relevant agency or an employee or agent of a person who has entered into a contract, agreement or arrangement with the agency.

349 *IS Act* (n 348) s 40C.

350 *IS Act* (n 348) s 40D.

351 *Australian Security Intelligence Organisation Act 1979* (Cth) ss 18A(1)(d) and 18B(1)(d) ('*ASIO Act*').

352 *Office of National Intelligence Act 2018* (Cth) ss 44(1)(a) and 44(2)(a).

6.14 These offences do not apply to all persons; only to those covered by the definition of staff member in the relevant Act (as well as ASIS agents and Australian Security Intelligence Organisation (ASIO) affiliates) and those with a 'contract agreement or arrangement' with the agency.[353]

The fault elements for 'dealing'

6.15 To be convicted of a 'dealing with' offence under the *Criminal Code*, and under the related Acts, the prosecution must show that the person dealt with the information and that they did so *intentionally*. The prosecution must also prove that the accused was *reckless* as to whether it was the type of information covered by the offence (for deemed harm) or to the harm or likely harm (for harm-based offences).

6.16 The definition of the fault (mental) element of recklessness is discussed in **Chapter 4**. Intention, which relates to physical elements such as 'receiving', is met if the person 'means to engage in that conduct'.[354] This is discussed further below.

6.17 There is no requirement that any harm result from the 'dealing' for the deemed harm offences in the *IS Act*, *ASIO Act* or *ONI Act* or in s 122.1(2) of the *Criminal Code*. The harm-based offence in s 122.2(2) of the *Criminal Code* requires the dealing to have caused harm or be likely to cause harm of the relevant type. The dealing with offence for non-officials is currently a mixture of deemed harm (s 122.4A(2)(d)(i) – classified information) and harm-based (s 122.4A(2)(d)(ii)-(iv)).

Submissions on 'dealing with' offences

6.18 Submissions on the 'dealing with' offences can be broadly divided into 3 categories: concerns about the breadth and uncertainty of the language used; concern about application of 'dealing with' offences to non-officials; and support for retaining dealing with offences.

Concern about breadth and uncertainty

6.19 There were differing views in submissions about when the fault (mental) element of intention to 'deal with' information would be satisfied. This was particularly evident when it came to discussions about when a person intentionally *receives* information.

---

353 As discussed in Chapter 1, the combination of the definition of Commonwealth officer and persons 'otherwise engaged to perform work for a Commonwealth entity' probably incorporates all, or almost all, of those people as well as many others.

354 *Criminal Code* (n 345) s 5.2.

6.20 The Attorney-General's Department (AGD) said that, in their view, 'unsolicited receipt or other unwitting dealings will not be sufficient to reach the threshold of intention'.[355] It is not clear exactly what 'unsolicited' means in this submission. For example, is a civil society group whose role includes receiving information directed at exposing human rights abuses 'soliciting' information about that topic? Similar questions arise in relation to journalists who report on defence and national security matters or to lawyers asking clients for information to advise them in a civil or criminal matter.

6.21 When the Parliamentary Joint Committee on Human Rights (PJCHR) was considering the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2018 (EFI Bill), it said that the inclusion of the term 'receive' in the definition of 'deals with' created a degree of 'uncertainty or confusion as to whether the person does or does not have the requisite intention with respect to conduct'.[356]

6.22 The Law Council of Australia said that intentionally receiving could be satisfied by merely opening an email:

> the fault element with respect to the physical element of dealing, which encompasses 'receiving' or 'obtaining' …, is intention – this only means that the physical act of receiving, for example, opening an email, is intentional.[357]

6.23 In relation to the fault (mental) element relevant to the kind of information (recklessness as to whether the information is in a particular category) there was some uncertainty as to whether a person is required to take active steps to avoid receiving certain information if they work in a field where that risk exists (for example, if they are a civil society group assisting whistleblowers or a journalist reporting on national security or defence matters). For example, the Law Council of Australia noted that 'dealing with' offence provisions may be enlivened by the knowledge of a substantial risk of receiving classified information:

> The mental element attaching to the physical element, of the information having a certain character, for example, that the information is security classified, is recklessness. This means it is sufficient if a person is aware of a substantial risk that they may receive security classified information and it is unjustifiable for them to take that risk.[358]

---

355 Attorney-General's Department (AGD), *Review of Secrecy Provisions* (Final Report, 21 November 2023) 38 [161]–[162] ('*AGD Review of Secrecy Provisions*'). See also AGD, *Submission 7*, [79].

356 Parliamentary Joint Committee on Human Rights (PJCHR), Parliament of Australia, *Human Rights Scrutiny Report* (Report No 3, 27 March 2018) ('*PJCHR Human Rights Scrutiny Report 3*') 228-229 [2.305]-[2.307].

357 Law Council of Australia, *Submission 19*, 39 [136].

358 Law Council of Australia, *Submission 19*, 39 [136].

6.24 AGD said that, in their view, it is not necessary for a person to act proactively to avoid receiving information; rather, it is an obligation 'not to intentionally engage in conduct where the substantial and unjustifiable risk of harm is known to the person'.[359]

6.25 The Australian Human Rights Commission noted the conclusions of the PJCHR on the definition of 'deal' and said that a positive obligation to proactively avoid receiving classified information would be inconsistent with the general principles of criminal responsibility.[360]

6.26 There were also submissions about the imprecision of drafting and potential unintended consequences. For example, the joint academic submission noted that the framing of the language in the definition of 'dealing with' information leads to offences that are potentially quite broad.[361] Similarly, the Human Rights Law Centre (HRLC) noted that the 'dealing with' provisions that apply to officials could impact on legitimate efforts to expose wrongdoing:

> It is readily imaginable that a public servant who otherwise blows the whistle properly and consistently with the PID Act could be prosecuted under dealing with offences in relation to prior conduct (such as photocopying and then taking home a document, to provide to an oversight body, or a journalist, in situations otherwise permitted under the PID Act).[362]

6.27 The Australian Law Reform Commission (ALRC) report *Secrecy Laws and Open Government in Australia* (ALRC 2009 Secrecy Laws Report) was clear that mere receipt or possession of information should not be covered in general secrecy offences.[363]

Concern about 'dealing with' offences applying to non-officials

6.28 There were many submissions raising concerns about the appropriateness of applying any form of 'dealing with' offence to non-officials. Some framed their concern as criminalising the legitimate activities of media and civil society groups. For example, the joint academic submission said that the offence could be enlivened by the use of an encrypted email account:

> If a journalist sets up an encrypted email account and makes a general invitation for people to send information about possible wrongdoing in government – a perfectly legitimate act for civil society actors concerned with the proper conduct of government – they could be criminally liable simply for receiving a classified document. If they then print out or email a

359 AGD, *Submission 7*, 17 [80].
360 Australian Human Rights Commission, *Submission 17*, 17 [64]–[65].
361 Joint Academic Submission, *Submission 13*, 6.
362 Human Rights Law Centre (HRLC), *Submission 14*, 7.
363 Australian Law Reform Commission (ALRC), *Secrecy Laws and Open Government in Australia* (Report No 112, December 2009) 203 [6.82], 224 [6.165] ('*ALRC 2009 Secrecy Laws Report*').

> copy and consult with an editor about what to do with it, they will have compounded the offence.[364]

6.29 Similarly, the Alliance for Journalists' Freedom (AJF) said that many journalists, academics and civil society groups use encrypted email services as a response to a perceived obligation to 'discourage current and former Commonwealth officers from providing them with information, lest they be guilty of soliciting restricted information' and that this type of requirement was not reasonable to 'impose on civil society members who are reasonably concerned with integrity of the security agencies and open, accountable government'.[365]

6.30 HRLC provided an example of how uncertainty about the operation of the provision affects their work:

> The Human Rights Law Centre actively promotes the availability of our Whistleblower Project to provide legal advice to potential whistleblowers. Say an intelligence officer was concerned about corruption within their agency, and wanted to speak up through appropriate channels. They contacted our Whistleblower Project through our intake portal, failing to observe our warnings that we cannot assist intelligence whistleblowers. Or, they may think, wrongly, that intelligence information is limited to actual sensitive information, not the much wider scope of the relevant definitions in section 41 of the PID Act. A junior lawyer at the Project receives the intake submission, and grows concerned that the information contained therein is intelligence information. There is, first, a very real possibility that this lawyer's mere receipt of the information could constitute an offence under the 'dealing with' offence in s 122.4A(2), with ss 90(1) and 121.1 together defining 'deal' as including to receive or obtain information. Seemingly, all the other elements of the s 122.4A(2) offence are satisfied. The s 122.5(4) defence in relation to the PID Act would not be available, given the blanket exclusions for intelligence whistleblowing in that law. Nor would the s 122.5(5A) defence arise, given the dealing with was not for the purpose of legal advice in relation to the operation of the Criminal Code itself, but in relation to reporting wrongdoing.[366]

6.31 The Media, Entertainment and Arts Alliance (MEAA) was also concerned that the 'dealing with' offences impinge on the legitimate activities of journalists:

> Journalists need to be able to ask for proof or evidence from sources – and in such cases, they may not know the classification or the content of the documentation in advance of having received it. Calculated decisions also need to be made about the public interest. Journalists need to see documents in order to evaluate whether something is in the public interest. Furthermore, journalists should be able to speak to lawyers to get advice and talk to relevant colleagues including lawyers about the status of that document. Undertaking these steps should not be considered a prosecutable offence.[367]

---

364 Joint Academic Submission, *Submission 13*, 15.

365 Alliance for Journalists' Freedom (AJF), *Submission 11*, [6.3].

366 HRLC, *Submission 14*, 8–9.

367 Media, Entertainment and Arts Alliance (MEAA), *Supplementary submission 22,* 3.

6.32 Several groups recommended that the 'dealing with' offences for non-officials be abolished or significantly narrowed. For example:

- AJF and the joint academic submission recommended that 'deal with' not include receipt of information by a non-Commonwealth officer.[368]
- MEAA believe that all of the 'dealing with' offences should be 'struck out in relation to journalists'.[369]
- The Law Council of Australia 'strongly opposes' any 'dealing with' offences for non-officials and considers them disproportionate.[370]
- HRLC recommended that dealing with offences for non-officials be abolished and the 'dealing with' offences for officials be confined to 'those in the public service, such as intelligence operatives, who are dealing with intelligence or national security information that is likely to have a significant impact on the public interest if disclosed'.[371]
- Australia's Right to Know (ARTK) was also of the view that the offence should be limited to only *disclosures* of information, not dealing with, because 'it is only disclosure of information that risks meaningful damage to essential public interests'.[372] ARTK also said that, if dealing with offences are retained, there should be a requirement for the prosecution to establish that the 'dealing with' was not in the public interest[373] (see also **Chapter 9**).

6.33 In 2009 the ALRC recommendation on 'dealing with' type offences for non-officials was that it be limited to circumstances where the disclosure from the Commonwealth officer to the non-Commonwealth officer was made on terms requiring it to be held in confidence and that the non-Commonwealth officer knows or is reckless to whether subsequent disclosure would harm an essential public interest.[374]

6.34 In my opening statement at the public hearing I expressed a preliminary view that 'dealing with' offences for non-officials should be removed or reduced

> At this stage of the review, I am minded to agree that – at the very least – merely receiving information should be removed from the offence. [375]

368 AJF, *Submission 11*, [6.3]; Joint Academic Submission, *Submission 13*, 15.
369 MEAA, *Supplementary submission 22,* 3.
370 Law Council of Australia, *Submission 19,* 38–40.
371 HRLC, *Submission 14*, 7–8.
372 Australia's Right to Know (ARTK), *Supplementary submission 21,* 9 [82].
373 ARTK, *Submission 12*, 16 [78].
374 *ALRC 2009 Secrecy Laws Report* (n 363) 222–225 [6.156]–[6.166].
375 Mr Jake Blight, INSLM, *Public hearing transcript*, 25 March 2024, 8.

6.35 In response, a number of non-government organisations made supplementary submissions that expanded on their reasons for supporting the abolition of 'dealing with' offences for non-officials.[376] For example, ARTK said

> It adds incoherence to the law to add what is in substance an 'attempt' offence in s 122.4A(2) by criminalising activity which is preparatory to the 'communication' of information and so already criminalised by s 122.4A(1).[377]

6.36 In relation to the argument that it is necessary to criminalise 'dealing with' by journalists because of the risk that a foreign intelligence agency may target a journalist to obtain that information, ARTK made the point that it is not normal in our legal system to penalise a person because a third party (such as foreign agent) may in future commit a criminal act:

> [In] our system of law, we do not criminalise conduct based on the suspicion that harm may be caused not by the defendant but by the further criminal act of some third party.
> The security agencies may take the view that harm may result from the aggressive and criminal actions of a third party hostile to the interests of the nation when a foreign intelligence agency seeks to exfiltrate data from a media organisation or physically penetrates the media company's business premises. However, it is an unacceptable extension of the principles of criminal liability to suggest that someone should be jailed for 2 years because there is a risk that the themselves may be the victim of a crime.[378]

Support for retaining 'dealing with' offences

6.37 Most intelligence agency submissions made broad statements in support of the retention of specific secrecy offences in the *IS Act*, *ASIO Act* and *ONI Act* without making a distinction between the act of communicating information and the act of 'dealing with' information.[379]

6.38 The Office of National Intelligence pointed to the Explanatory Memorandum to the *ONI Act* as evidence that the 'dealing with' provisions of the Act contain an appropriate penalty in proportion to the 'sensitive nature of the information put at risk, which may jeopardise Australia's national security'.[380]

---

376 ARTK, *Supplementary submission 21*, 9-10 [81]–[89]; MEAA, *Supplementary submission* 22, 3; Law Council of Australia, *Supplementary submission 26*, 2–3.

377 ARTK, *Supplementary submission 21*, 9 [83].

378 ARTK, *Supplementary submission 21*, 10 [88]–[89].

379 See ASD, *Submission 4*, 4 [6]; Defence Intelligence Group, *Submission 5*, 2 [7]; ASIS, *Submission 10*, 8 [39]. The Australian Security Intelligence Organisation (ASIO) indicated it saw good reasons for maintaining the secrecy offences in the *ASIO Act* but acknowledged there might be other ways address their objectives: ASIO, *Submission 6*, 5 [28].

380 Office of National Intelligence, *Submission 8*, 11.

6.39 ASIO took a more considered position. At the public hearing, Mr Mike Burgess, Director-General of Security, suggested that an offence for mere receipt by a non-official was not necessary or at least not effective as a deterrent:

> in terms of your specific question of mere receipt: secrecy provisions are here for deterrence purposes. Once someone's received something, then the deterrence has not had its effect. So mere receipt perhaps should not be. And that's not the issue as far as I'm concerned. It's what happens next. As you remarked in your opening statement, of course, if then someone decides to hold on to something and keep it for reasons which are not defendable, and start communicating it to others, that's the problem that we need to focus on.[381]

6.40 None of the intelligence agencies made supplementary submissions about the 'dealing with' offences in response to the preliminary view expressed in my opening statement at the public hearing.[382]

Findings on 'dealing with' and officials

6.41 I accept that there are situations where harm can arise from 'dealing with' information because it makes information vulnerable to theft by foreign intelligence agencies. I am also cognisant that it is not a normal part of our legal system to penalise a person's actions because of the risk that a third party might commit an offence. However, for Commonwealth officers and people otherwise engaged to perform work for a Commonwealth entity, there is a good argument that, because of their special position and the duties they have voluntarily taken on, it is reasonable to impose criminal penalties for recklessly dealing with certain official information in a way that puts the information at particular risk. However, even for officials, the current definition of 'deal' is unnecessarily broad and complex.

6.42 Merely receiving information should not be part of any 'dealing with' offence, even for officials. It is neither necessary to address the potential harm underlying the secrecy offences nor proportionate, particularly having regard to its broad application. Further, as Mr Burgess said, penalising receipt is not an effective deterrent to the original disclosure.

6.43 The term 'obtain' overlaps with 'receive'.[383] While 'collect' and 'possess' both imply an active step this is not necessarily the case with 'obtain' and there is a risk that a person could obtain something simply by being given it by another person. Obtain should also be removed from the definition. In the situation where an official actively gathers documents they will have 'collected' them and this should remain in the offence.

---

381 Mr Mike Burgess, Director-General of Security, *Public hearing transcript*, 25 March 2024, 17.

382 Mr Jake Blight, INSLM, *Public hearing transcript*, 25 March 2024, 8.

383 The Macquarie Dictionary defines the verb *obtain* as 'to come into possession of; get or acquire; procure, as by effort or request'. See *Macquarie Dictionary* (online at 27 May 2024) 'obtain'.

6.44 The parts of the definition that overlap with disclosure offences (communicating, publishing and making available) should be removed, as they are not necessary and only add confusion to the operation of the offences.

6.45 It is not clear that the 'alter and conceal' parts of the definition are necessary or proportionate. For harm to occur, the person would also need to do at least one of the other things in the definition (collect, possess, record or copy) or communicate the information. If they were 'altering or concealing' as part of attempting to communicate information or committing any other ancillary offence then that would also already be an offence.

6.46 For an official or person otherwise engaged to perform work for the Commonwealth acting without authority, the remaining parts of the definition (collect, possess, record, copy) are broadly justifiable, but some clarification may be needed to ensure that possession does not include mere receipt from another person. Consideration could be given to whether the language used in the *IS Act* and other intelligence legislation might be a useful model, although without the 'any other manner' category. On that model, dealing would be copying, transcribing, retaining or removing records, as well as making a record of any information or matter that came to the knowledge of the person in the course of their work as a Commonwealth officer or person otherwise engaged to perform work for a Commonwealth entity.

RECOMMENDATION 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.

6.47 As noted above, the definition of 'deal' for Part 5.6 cross-refers to the definition of 'deal' for Part 5.2 of the *Criminal Code*. My comments here on the definition of 'deal' relate only to the Part 5.6 offences of the *Criminal Code*. The definition of 'deal' for the offences in Part 5.2 (espionage and foreign interference) of the *Criminal Code* will be considered in the INSLM review on Part 5.2.

Findings on 'dealing with' and non-officials

6.48 I have considered carefully the evidence put forward in submissions to the review, and in evidence at the public hearing, on matters related to 'dealing with' information in ss 122.1(2), 122.2(2) and 122.4A(2) of the *Criminal Code*. It is clear that journalists, academics and civil society groups hold a significant degree of concern about what it means to 'deal with' information, including the more uncertain aspects of the definition that criminalise actions such as the receipt of information. These concerns are having an impact on the way some civil society groups and journalists go about their work.

6.49 It is important to remember that 'dealing with' offences operate alongside the usual ancillary offences for aiding, abetting, inciting, conspiring and so on. This means that it is not necessary for 'dealing with' offences to cover situations where, for example, a journalist actively incites or conspires with an official to have the official communicate intelligence information. Also, it is not necessary for a general 'dealing with' offence to cover situations where a person deals with information in order to prepare for espionage or foreign interference, as these are already separate offences.

6.50 I acknowledge that any time information that could harm the national interest is taken outside the extremely secure buildings and systems used by intelligence agencies, there is some risk that it could fall into the hands of a person or entity that may seek to harm those national interests.[384] However, it does not necessarily follow that the criminal law should impose the same sort of obligations on non-officials as it does on officials. Non-officials do not have the same sort of duty to protect the national interest by preventing third parties from committing crimes that officials arguably do. Criminal law must also take account of the proportionality of the penalty to the harm caused and the expected knowledge of harm a non-official could reasonably be expected to hold.

6.51 Several other reviews have also come to conclusion that information offences for officials and non-officials should recognise the different position of non-officials, even when the risk of harm is much the same.[385] There is further discussion on principles for offences for non-officials in **Chapter 8**.

6.52 In other Five Eyes countries where offences for non-officials using, communicating and retaining information exist, they require not only harm but also an intention or knowledge that the harm will occur or at least a reasonable belief specific harm will occur. Further information about these offences is in **Chapter 8**.

6.53 I have already stated that the offence of 'receiving' information should be removed from any 'dealing with' offence, as it is neither necessary nor proportionate. That is even more so for non-officials, who have no general duties to the Commonwealth and should not have to take active steps to avoid receiving information that might be the subject of a secrecy offence.

6.54 More broadly, it is difficult to see how any 'dealing with' offences can be justified as necessary and proportionate for non-officials. This is particularly so when other offences already apply

---

384 I acknowledge the evidence received from Mr Robert Todd, ARTK, and Mr Paul Farrell, MEAA, at the public hearing that media groups take great care to protect their sources and to ensure that information is not disclosed unintentionally. However, I also recognise that there is a risk that actors such as some foreign intelligence agencies possess sophisticated tools that they seek to deploy to extract information from systems, including those subject to heightened security measures.

385 See, for example, the discussion in the ALRC 2009 Secrecy Laws Report (n 363) 191 [6.29] and Roger Gyles, INSLM (former), *Report on the Impact on Journalists of Section 35P of the ASIO Act* (Report, October 2015) 22-23 [42].

in circumstances where criminal culpability arises. For example, the offences of inciting and conspiring apply where a non-official actively encourages an official to commit a disclosure offence. If the 'dealing with' is on behalf of a foreign principal or for espionage, there are different offences that apply. Depending on the specific facts, it is possible that possession of stolen property offences may also apply. On balance, I recommend that the 'dealing with' offences be removed for non-officials. Ancillary offences (such as inciting or conspiring) should continue to apply.

RECOMMENDATION 8: The offence for 'dealing with' information by non-officials in s 122.4A(2) should be repealed.

Proper place of custody offences

6.55 Part 5.6 of the *Criminal Code* makes it an offence for a current or former Commonwealth officer or other person engaged to perform work for the Commonwealth to remove or hold certain information outside of the 'proper place of custody'.[386] The definition of 'proper place of custody' has the meaning prescribed by the regulations.[387]

6.56 These offences are not operational because, in the almost 6 years since the enactment of the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth) (*EFI Act*), no such regulations have been made.

6.57 The AGD *Review of Secrecy Provisions* report recommended the repeal of the proper place of custody offences in ss 122.1(3) and 122.2(3) of the *Criminal Code:*[388]

> The Review understands efforts have been made over the five years since these offences were enacted to define 'proper place of custody' and that Commonwealth agencies have been unable to agree on a definition that does not impose a disproportionately high and onerous burden on public servants.
>
> The Review also notes that, as discussed above, 'dealing' with information is defined broadly for the purposes of the general secrecy offences. The Review is satisfied that the dealing offences would cover the conduct that is the subject of the proper place of custody offence such that, if the proper place of custody offences were repealed, there is unlikely to be a gap.[389]

386 *Criminal Code* (n 345) ss 122.1(3), 122.2(3).
387 *Criminal Code* (n 345) s 121.2.
388 *AGD Review of Secrecy Provisions* (n 355) 41 [177]–[181].
389 *AGD Review of Secrecy Provisions* (n 355) 41 [178]–[179].

6.58 The Law Council of Australia agreed with the conclusion of the AGD Review of Secrecy Provisions.[390]

6.59 The proper place of custody offences should be repealed. Regulations to give effect to these offences have never been made, indicating that the offences are not necessary. Copying and removing relevant information without authority is likely to be covered by the 'dealing with' offences for Commonwealth officials. Other offences, including theft of Commonwealth property, failure to comply with a direction and preparatory offences for foreign interference and espionage offences, may also apply depending on the facts.

RECOMMENDATION 9: The 'proper place of custody' offences in ss 122.1(3) and 122.2(3) should be repealed.

Failure to comply with a direction offence

6.60 Those who obtain relevant information in their capacity as a current or former Commonwealth officer or other person engaged to perform work for a Commonwealth entity are subject to additional offences under s 122.1(4) if they do not comply with a lawful direction regarding the retention, use or disposal of 'inherently harmful information' and the result is a 'risk to the security of the information'. A similar offence exists in s 122.2(4) for directions regarding the retention, use or disposal of other information where doing so 'causes harm to Australia's interests' or is likely to 'cause harm to Australia's interests'.

6.61 The examples of lawful directions given in the Revised Explanatory Memorandum all relate to *specific* directions given to one person by another.[391] It is not entirely clear if the offence is intended to cover broad directions to classes of people (for example, a direction to all security clearance holders to comply with all of the policies made under the Protective Security Policy Framework (PSPF)). However, there would be real doubts about whether a direction of this kind would be a lawful direction because of its breadth and uncertainty. It

390 Law Council of Australia, *Submission 19*, 28.

391 See, eg, Revised Explanatory Memorandum, National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 (Cth) 242 [1403] that gives the following example: Person A is employed under the *Members of Parliament (Staff) Act 1984* (Cth). Person A is given a document containing an update on an ongoing criminal intelligence investigation by Person B, a senior official of the Australian Criminal Intelligence Commission (ACIC). The document contains information obtained using the ACIC's coercive examination powers and from a source. Person B directs Person A to store the document in a safe that only Person A has access to. Person A stores the document in a safe that is accessible by all staff in the office. See also 243 [1409]–[1413], 255 [1487].

will be a question of fact to be proved that a person had authority to give the direction and that the direction was lawful.

6.62 The power to give a lawful direction is most commonly associated with employment. Commonwealth officers who fail to comply with a lawful direction, even where doing so does not result in harm, are also liable to be subject to disciplinary action under the *Public Service Act 1999* (Cth), *Defence Force Discipline Act 1982* (Cth) or other applicable legislation.

6.63 The Director-General of Security noted in evidence that there would be utility in retaining a 'lawful directions' provision for former officials where it would enable the protection of 'information which must be protected under law'.[392] It is not clear to me what the source of the power to give a lawful direction to a former official or contractor would be. It is possible that such a power might arise under contract (for example, if a contract of engagement provides for the Commonwealth to give directions about information that was provided during the term of contract even after the contract has ceased).

6.64 No further submissions or evidence was received on these offences.

6.65 These offences are of relatively narrow scope. It is reasonable and proportionate for the Commonwealth to be able to give lawful directions to its own officials about information that the person has made or obtained by reason of being a Commonwealth official. Importantly, both offences about compliance with lawful directions have a harm element or at least a risk of harm element (albeit, for inherently harmful information, the risk is to do with security of the information).

6.66 On this basis, I do not recommend any changes to the lawful direction offences at this point.

Aggravated offences

6.67 Section 122.3 provides 4 circumstances in which an offence by a Commonwealth officer (or other person otherwise engaged to perform work for the Commonwealth) against ss 122.1 or 122.2 becomes an aggravated offence:

> (ii) if the commission of the underlying offence involves a record – the record is marked with a code word, "for Australian eyes only" or as prescribed by the regulations for the purposes of this subparagraph;
> (iii) the commission of the underlying offence involves 5 or more records each of which has a security classification;
> (iv) the commission of the underlying offence involves the person altering a record to remove or conceal its security classification;

392 Mr Mike Burgess, Director-General of Security, ASIO, *Public hearing transcript,* 25 March 2024, 17.

(v) at the time the person committed the underlying offence, the person held an Australian Government security clearance allowing the person to access information that has a security classification of at least secret.[393]

6.68 Section 122.3 applies to each of the offences in ss 122.1 and 122.2. If one of these offences becomes an aggravated offence, the penalty increases: a 7-year offence increases to 10 years; and a 3-year offence increases to 5 years.

6.69 Before discussing each of these aggravating factors, it is useful to mention the AGD *A Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* (Guide to Framing Commonwealth Offences) and to very briefly discuss the sorts of aggravating factors already considered in sentencing.

Guide to Framing Commonwealth Offences

6.70 The Guide to Framing Commonwealth Offences provides policy guidance on the types of things to be considered when drafting or changing offences under Commonwealth law.

6.71 Although it does not expressly refer to 'aggravated offences' or provide general principles underpinning their construction, in its guidance on 'setting an appropriate penalty' it states:

> A higher maximum penalty will be justified where there are strong incentives to commit the offence, or where the consequences of the commission of the offence are particularly dangerous or damaging.[394]

6.72 This suggests that the creation of an aggravated offence is indicated where the consequences of the offence are particularly dangerous or damaging. Offences in other parts of the *Criminal Code* indicate that aggravated offences generally reflect a significant escalation in the conduct or the actual or likely harm caused by the basic offence.[395]

6.73 In a submission to this review, AGD said that 'the graduation in penalties for aggravated offences should reflect the relative seriousness of the conduct involved, in line with the principles in the Guide'.[396]

---

393 The circumstances in s 122.3(1)(b) start from the number (ii) – this reflects the absence of a fifth circumstance numbered (i), which was removed before the Act commenced.

394 AGD, *A Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* (Guideline, September 2011) 38 [3.1.1] ('*Guide to Framing Commonwealth Offences*').

395 See, eg, *Criminal Code* (n 345*)* ss 71.13, 73.1–3, 127.1A(1)(b), 132.3.

396 AGD, *Submission 7*, 9 [39].

Sentencing principles

6.74 Section 16A(2) of the *Crimes Act 1914* (Cth) provides a non-exhaustive list of matters that judges must have regard to when determining a sentence. Further, general common law principles may give content to the central requirement imposed by s 16A(1) that a court sentencing a federal offender must impose a sentence or make an order that is of a 'severity appropriate in all the circumstances'.[397]

6.75 There are a number of matters in s 16A(2) of the *Crimes Act* which are relevant to secrecy offences. These include:

- the nature and circumstances of the offence.[398] This includes a wide range of matters. Some examples are the extent of any planning or premeditation; the degree of sophistication; the danger posed or harm caused to others; whether it involved a breach of trust or abuse of position; whether it was of a kind that was difficult to detect or prosecute; any steps taken to avoid detection or to destroy or conceal evidence; the offender's state of mind; the role played by the offender; and whether the role ceased voluntarily or ceased only because of investigation or detection[399]
- the offence forms part of a course of conduct consisting of a series of criminal acts of the same or a similar character[400]
- any injury, loss or damage resulting from the offence.[401]

6.76 These sorts of aggravating circumstances are routinely, and appropriately, matters of discretion for the sentencing judge. Only in special circumstances do they need to be dealt with separately in an enactment.

Statutory aggravating circumstances

6.77 Having very briefly discussed the Guide to Framing Commonwealth Offences and general sentencing principles I now turn to the specific statutory aggravating circumstance in s 122.3.

For Australian eyes only

6.78 The first of the aggravating circumstances in the current s 122.3 is that the 'record is marked with a code word, "for Australian eyes only" or as prescribed the regulations'. No other code words have been prescribed. Beyond this, the *Criminal Code* does not require that a code

397 Commonwealth Director of Public Prosecutions, *Sentencing of Federal Offenders in Australia: A Guide for Practitioners* (Guideline, 6th ed, April 2023) 39-40 ('*CDPP Sentencing Guidelines*').
398 *Crimes Act 1914* (Cth) s 16A(2)(a).
399 *CDPP Sentencing Guidelines* (n 397) 46 [216].
400 *Crimes Act* (n 398) s 16A(2)(c).
401 *Crimes Act* (n 398) s 16A(2)(e).

word be applied in accordance with any particular criteria or relate to any particular threshold of harm.

6.79 The wording of s 122.3(b)(ii) is somewhat ambiguous – it is unclear whether s 122.3(b)(ii) applies to any 'code word' *as well as* a marking of 'for Australian eyes only' (or as prescribed by regulation) or whether it applies to the code word 'for Australian eyes only' (plus any prescribed by regulation).

6.80 If it meant any 'code word' (and not just 'for Australian eyes only' plus any prescribed by regulation) then that would create significant uncertainty, grant an excessively broad discretion to the executive to determine an element of the criminal law (and a penalty) and make the law 'unknowable', as there would be no requirement to publish the code words that made an offence aggravated. The reasons these outcomes would be contrary to general rule of law principles are discussed in **Chapter 4.**

6.81 Even if s 122.3(b)(ii) is intended to be limited to 'for Australian eyes only' and code words prescribed in the regulations, there are still significant problems with this circumstance.

6.82 In practice, records are not usually marked with the actual words 'for Australian eyes only'. However, they are sometimes marked with the releasability caveat 'AUSTEO'. It is not clear that a document marked 'AUSTEO' would actually meet the requirement of s 122.3(b)(ii) because the *Criminal Code* only refers to the marking of 'for Australian eyes only'.

6.83 It might be assumed that the PSPF will guide officials on when to use code words. It does contain reference to a number of code words. The PSPF provides very little guidance on the criteria for applying AUSTEO (which is described as a caveat), simply stating:

> The AUSTEO caveat indicates only appropriately cleared Australian citizens can access the information. Additional citizenships do not preclude access. Information marked AUSTEO is only passed to, or accessed by, Australian citizens. While a person who has dual citizenship may be given AUSTEO-marked information, in no circumstances may the Australian citizenship requirement be waived.[402]
>
> If there is a business need to share AUSTEO information with a person who is not an Australian citizen, the originator can, on a case-by-case basis, reconsider application of the AUSTEO caveat to its information and, if warranted, apply a different caveat or classification to that information (e.g. the AGAO or REL caveat).[403]

---

402 Department of Home Affairs, *Protective Security Policy Framework, Policy 8: Classifications System* (Policy No 8, August 2023) 12 ('*PSPF Policy 8*'). No additional guidance on when the marking is to be applied is included in the *Australian Government Security Caveat Guidelines* (Caveat Guidelines) which officials are to comply with in accordance with requirement 6 of *PSPF Policy 8*. The Caveat Guidelines are not publicly available (see Chapter 4).

403 Department of Home Affairs, *Protective Security Policy Framework, Policy 9: Access to Information* (Policy No 9, January 2024) 4 [18].

6.84 This guidance on the use of AUSTEO does not satisfy the criteria in the Guide to Framing Commonwealth Offences for a higher maximum penalty that consequences of the commission of the offence are particularly dangerous or damaging. It only states that AUSTEO information should only be accessed by Australian citizens. In accordance with the PSPF and the *Australian Government Security Caveat Guidelines* (Caveat Guidelines), AUSTEO marking can be applied to information which has a classification of less than secret. The Caveat Guidelines and annex are not publicly available (see discussion in **Chapter 4**).

6.85 The aggravating circumstance that a record is marked with a code word should be removed. It is uncertain, gives excessive discretion to the executive, is 'unknowable' in so far as non-public policies are involved and is also not a sufficiently clear indicator of additional harm.

6.86 This does not mean that additional harm that might arise as a matter of *fact* cannot be considered as part of the ordinary sentencing principles (discussed above). Also, it does not mean that the presence of a code word or caveat may not be relevant to establishing the recklessness of an official who disclosed information with a code word or caveat marking on it. Further discussion on how the layout, format and markings of documents can assist in establishing recklessness is in **Chapter 4**.

Five records or more

6.87 The second of the current aggravating circumstances is that the underlying offence involve 5 or more records, each of which has a security classification.

6.88 For the reasons discussed in **Chapter 4**, classification markings should not be part of an offence. That reasoning also applies to an aggravated offence.

6.89 Leaving aside the reference to the classification markings, and focusing on the number of records, there are certainly some circumstances where the disclosure of a large volume of material can cause significant damage. HRLC suggested that this provision contemplates an 'Edward Snowden-type scenario where a high volume of classified documents might be leaked indiscriminately'.[404]

6.90 However, as the joint academic submission pointed out, the threshold of 5 or more records is arbitrary and not necessarily reflective of the harm risked or caused, because one document could easily be more harmful than 5 or more depending on their content:

> Depending on its content, 1 security classified document released publicly could be sufficient to cause grave damage to national security; 5 documents, or 10, or 100, could cause far less harm if they contain information of less consequence. In other words, the quantity of

404 HRLC, S*upplementary submission 23*, 2.

documents involved in the offence does not directly correlate with the level of harm to be caused.[405]

6.91 As the joint academic submission also pointed out, that threshold is particularly arbitrary in circumstances where multiple electronic records can easily be 'dealt with' in an instant in today's digital age.[406]

6.92 Disclosures of multiple pieces of harmful information or multiple disclosures can already be dealt with in 2 ways: first, through ordinary sentencing principles (discussed above), including where disclosure of multiple pieces of information causes more harm; and, second, where appropriate, by indicting a defendant with multiple charges under ss 122.1 and 122.2 if they have made a series of disclosures.[407]

6.93 As the aggravating circumstance of 5 or more records is arbitrary and not necessarily linked to increase in harm, it should be repealed.

6.94 Where an individual has dealt with or communicated multiple records, this may point to an *intention* to or cause the harm. This is a stronger indicator of aggravation than an arbitrary number of records. This is discussed further below as a possible reason to increase the penalties.

Alter, conceal or remove security marking

6.95 The third of the current aggravating circumstances is that the person 'alter[s] a record to remove or conceal its security classification'.

6.96 It is not clear that altering or concealing will actually cause the underlying offence (disclosing or dealing) to be significantly more dangerous or damaging. It might, perhaps, have the result that the person to whom information is disclosed (such as a journalist) does not realise its sensitivity, and this may lead to further disclosure. But this is a step removed from the conduct constituting the offence. It is also somewhat confusing that 'altering' and 'concealing' are already part of the existing 'dealing with' offences (although I have made recommendations about this above).

6.97 The Revised Explanatory Memorandum said that 'A person who takes … active steps to facilitate and conceal the commission of the underlying offence demonstrates a particularly

405 Joint Academic Submission, *Submission 13*, 6.
406 Joint Academic Submission, *Submission 13*, 5.
407 However, see *Crimes Act* (n 398) s 4C – each action can only be punished once.

high level of culpability, justifying a higher maximum penalty'.[408] This may be true, but deceptive conduct is a normal part of the sentencing principles and it is not clear why it should be treated differently in these circumstances. Alteration, concealment or removal of a security marking may also indicate premeditation to the offence.[409] Again, this is a factor that is routinely considered in ordinary sentencing principles.

6.98 The joint academic submission noted that one result of the provision could be to punish a person who, in order to 'deal with' information as per ss 122.1(2) and 122.2(2), conceals its security marking but ultimately chooses not to copy, remove or disclose it. It is not proportionate that this type of action be considered more serious and subject to a higher maximum penalty than the action of dealing with information *intending* to cause serious harm without first concealing or altering it.[410]

6.99 In the context of dealing and disclosure offences matters of dishonesty, fraud and premeditation do not amount to significantly more *damaging* or dangerous conduct and should not be an aggravated offence. They are nevertheless serious matters that go to *culpability* and are properly dealt with at sentencing in accordance with normal sentencing principles. They may also be relevant to intention to cause harm. This is discussed below.

Holding a security clearance

6.100 The fourth current aggravating circumstance is that at the time the person committed the underlying offence they held a security clearance enabling them to access information that has a security classification of at least secret.

6.101 Officials who have access to the type of information described in ss 122.1 and 122.2 (see **Chapters 4** and **5**) will, in almost all cases, have a security clearance allowing them to access information of at least secret (this is a PSPF requirement). The practical effect of this aggravating circumstance is therefore to make almost every offence under ss 122.1 and 122.2 an aggravated offence. This clearly does not meet the test in the Guide to Framing Commonwealth Offences of the consequences of the commission of the offence being *particularly* dangerous or damaging.

6.102 However, this does not mean that some kind of aggravating circumstance linked to security clearance is inappropriate if there is a category of clearance holders that is significantly

408 Explanatory Memorandum, National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 (Cth) 306 [1538].

409 Dr Keiran Hardy, Griffith University, *Public hearing transcript,* 25 March 2024, 44.

410 Joint Academic Submission, *Submission 13*, 6.

different from other clearance holders. The question of whether there is such a category was tested at the public hearings.

6.103 The Director-General of Security, Mr Burgess, agreed that holders of the highest level of security clearance (presently known as Top Secret Positive Vetting or Top Secret Positive Assurance) are in a distinct category of Commonwealth officials with access to the most sensitive information the Commonwealth holds. They will also likely have access to far more of it than holders of other clearances.[411] Following recent changes to the *ASIO Act*, these clearances will be managed by ASIO rather than Australian Government Security Vetting Agency because of their extreme sensitivity.[412]

6.104 Deputy Secretary of National Security and Resilience in the Department of Home Affairs, Mr Nathan Smyth, agreed that holders of the highest level of clearance are in a qualitatively different category to other officials.[413]

6.105 The Deputy Secretary of National Security and Criminal Justice Group from AGD, Ms Sarah Chidgey, questioned whether it would be sufficient to raise the 'bar' for a clearance as an aggravating factor to a clearance to access top secret information. However, Ms Chidgey also accepted that it could be argued that raising it to the highest level of clearance holders would put the offence on par with the offences specific to intelligence officials in terms of a position of trust.[414]

6.106 Commonwealth officials who hold the highest level of security clearance are trusted in a way that is qualitatively and quantitively different from officials who hold a lower-level clearance (or no clearance at all). These types of clearances involve a much greater degree of vetting and are not granted lightly. Those who have them have the highest level of access to the Commonwealth's most sensitive information and to greater quantities of information. This can include direct and unescorted access to areas and to electronic systems where the most sensitive information is held. There is also a particular harm to the Commonwealth and also to its relationship with foreign partners that occurs from a breach of trust by those granted the very highest level of clearance by the Commonwealth.

6.107 The aggravating circumstance for officials who held a security clearance at the relevant time of the offending should be retained, but the level of clearance should be changed to the highest level of security clearance. This is presently the clearance known as Top Secret Positive Assurance. ASIO grants this clearance in accordance with its security vetting

411 Mr Mike Burgess, Director-General of Security, ASIO, *Public hearing transcript*, 25 March 2024, 12.

412 *Australian Security Intelligence Organisation Amendment Act 2023* (Cth); ASIO, Submission No 1 to Parliamentary Joint Committee on Intelligence and Security (PJCIS), Parliament of Australia, *Review of the Australian Security Intelligence Organisation Amendment Bill 2023* (April 2023) 2.

413 Mr Nathan Smyth, Department of Home Affairs, *Public hearing transcript,* 25 March 2024, 83.

414 Ms Sarah Chidgey, AGD, *Public hearing transcript*, 26 March 2024, 150–151.

functions under the *ASIO Act*. Appropriate transitional provisions should ensure that the previous equivalent (Top Secret Positive Vetting clearances granted by Australian Government Security Vetting Agency or other agencies) are also covered.

Other possible aggravating circumstances

6.108 In addition to considering the 4 current aggravating circumstances discussed above, I have also considered whether there are other circumstances that warrant an increased penalty for secrecy offences by Commonwealth officers and other persons engaged to perform work for a Commonwealth entity.

6.109 HRLC recommended that an appropriate indicator of aggravation may be where 'serious harm' was caused by the disclosure.[415] If amendments to ss 122.1 and 122.2 are made in line with **Recommendations 1–3** and **6**, these offences will be limited to circumstances that will almost always result in serious harm. If exceptionally grave harm occurs, this can be addressed through normal sentencing principles.

6.110 The Australian Federal Police (AFP) suggested the inclusion of an additional aggravated circumstance where the information disclosed involves foreign equities or information from a foreign partner. It reasoned that the disclosure of this type of information could have significant implications for Australia's international relationships.[416] This information is already captured by ss 122.1 and 122.2 (**Recommendations 2** and **6**). Indeed, proposed definitions for **Recommendation 6** potentially broaden the types of international information sharing arrangements covered by the offence. As noted in **Chapter 3**, Australia's obligations under international information sharing agreements are to treat partner information equally, not place it in a special category. No different treatment should be given to 'partner information' in Part 5.6.

6.111 I also strongly reject AFP's proposal that consideration be given to the use of a conclusive certificate issued by an agency head or Minister to prove whether information includes content provided by a foreign partner.[417] I note that, in its original consideration of the EFI Bill, the Parliamentary Joint Committee on Intelligence and Security also rejected the proposal to include conclusive certificates for classified information.[418] It is inappropriate for conclusive certificates to be issued where the evidence the defendant would need to rely on to challenge the certificate would be in the control of the Commonwealth and where the

---

415 HRLC, *Submission 14*, 11, recommendation 9.

416 Australian Federal Police (AFP), *Submission 18*, 11–12.

417 AFP, *Submission 18*, 12.

418 PJCIS, *Advisory Report on the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (Report, June 2018) 76 [3.169].

certificate could be used to circumvent the need for the prosecution to make out a significant element of the aggravated offence. In line with the principles of the AGD Guide to Framing Commonwealth Offences*:*

> Evidentiary certificate provisions are generally only suitable where they relate to formal or technical matters that are not likely to be in dispute but that would be difficult to prove under the normal evidential rules, and should be subject to safeguards.[419]

6.112 Another circumstance where a higher penalty could be considered is where a person *intended* or *knew* their conduct would or was likely to cause the types of harm covered by ss 122.1 and 122.2.

6.113 This approach was suggested in the joint academic submission.[420] It aligns with the view put forward by the Law Council, ALRC and others that offences should cascade in penalty according to the culpability of the offender.[421]

6.114 I agree with this proposal. An additional penalty is appropriate where the offences in s 122.1 or s 122.2 are undertaken with knowledge or intention – even where the ultimate harm is the same. An additional 3-year penalty for disclosure offences and 2 years for 'dealing with' offences would be consistent with the current approach. Whether this is described as an aggravating offence or a separate offence is a drafting matter. If it is a separate offence then provision for an alternative verdict for recklessness would be appropriate.

RECOMMENDATION 10: 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 where the person intended or knew their conduct would or was likely to cause a type of harm covered by the underlying offence.

419 *Guide to Framing Commonwealth Offences* (n 394) 54.

420 Joint Academic Submission, *Submission 13*, 6. See also: Roger Gyles, INSLM (former), *Report on the Impact on Journalists of Section 35P of the ASIO Act* (Report, October 2015) 3.

421 Law Council of Australia, *Submission* 19, 10–27; ALRC, *Submission 3*.

Chapter 7: General secrecy offence

7.1 As discussed in **Chapters 4** and **5**, ss 122.1 and 122.2 of the *Criminal Code Act 1995* (Cth) are primarily concerned with national security, defence, international relations and law enforcement related information. In contrast, s 122.4 contains a broader secrecy offence that currently applies to current or former Commonwealth officers and people otherwise engaged to perform work for a Commonwealth entity who have a specific 'duty' not to disclose information. That 'duty' is not imposed by s 122.4 but must arise elsewhere. According to the Attorney-General's Department (AGD), this provision currently attaches criminal liability to 295 non-disclosure duties across Commonwealth law.[422] Section 122.4 was originally due to sunset in December 2023, but this has been extended to 29 December 2024.[423]

Section 70 of the *Crimes Act 1914*

7.2 When Part 5.6 of the *Criminal Code* was enacted it replaced ss 70 and 79 of the *Crimes Act 1914* (Cth). Section 70 of the *Crimes Act* was similar to s 122.4 in that both pertain to a broad class of information that officials come into contact with in the course of their work and neither contains an express harm element. The former s 70 of the *Crimes Act* made it an offence for a Commonwealth officer or a former Commonwealth officer to publish or communicate 'any fact or document which comes into his or her knowledge or into his or her possession by virtue of being a Commonwealth Officer'. This covered official information received or collected by the Commonwealth government as well as information generated within government.

7.3 The offence in s 70 was first enacted in 1914. In 1960 it was amended to extend to former Commonwealth officers. Apart from a few more minor amendments, the provision remained largely unchanged until 2018.

7.4 Section 70 was frequently criticised. Key critiques included:

- The provision appeared to criminalise any, even innocuous, disclosures of official information.[424]

422 Attorney-General's Department (AGD), *Submission 7*, 3 [4].

423 *Counter-Terrorism and Other Legislation Amendment Act 2023* (Cth).

424 Justice Susan Kenny, 'Secrecy Provisions: Policy and Practice' (Speech, National Information Law Conference, 24 March 2011) 11; John McGinness, 'Secrecy Provisions in Commonwealth Legislation' (1990) 9(1) *Federal Law Review* 49, 54.

- The scope and definition of information captured was unclear and 'unsatisfactory'.[425]
- There were doubts as to its compatibility with the implied freedom of political communication.[426]
- The offence did not require the prosecution to demonstrate any harm to a public interest.[427]

7.5 Whether such an offence should even exist at all was debated. Commentators voiced serious doubts about the need for criminal penalties to protect government information.[428] Agreeing with the Australian Law Reform Commission (ALRC) report *Secrecy laws and Open Government in Australia* (ALRC 2009 Secrecy Laws Report) (discussed below), Dr Keiran Hardy and Professor George Williams suggested that civil remedies such as suspension or termination of employment for breach of contract or confidentiality would be more suitable for breaches of common law statutory duties not to disclose. They argued that the unsuitability of criminal sanctions is particularly pertinent where there is a lack of harm or where there is no intention to cause harm.[429]

7.6 In its 1983 review, the Australian Human Rights Commission (AHRC) found that s 70 operated in a manner inconsistent with art 19 of the *International Covenant on Civil and Political Rights* (ICCPR).[430] See **Chapter 3** for a discussion of art 19.

7.7 Decades later, in its ALRC 2009 Secrecy Laws Report, the ALRC recommended the repeal of wide 'catch-all' secrecy provisions like s 70 and the introduction of a new 'general secrecy offence' that protected a narrowly defined category of 'essential public interests'. These harms were defined as unauthorised disclosures that are likely to:

- damage the security, defence or international relations of the Commonwealth
- prejudice the prevention, detection, investigation, prosecution or punishment of criminal offences
- endanger the life or physical safety of any person

---

425 McGinness (n 424) 72.

426 Keiran Hardy and George Williams, 'Terrorist, Traitor, or Whistleblower? Offences and Protections in Australia for Disclosing National Security Information' (2014) 37(2) *UNSW Law Journal* 784, 803.

427 Daniel Stewart, 'Simplifying Government Secrecy?' in Ron Levy, Molly O'Brien, Simon Rice, Pauline Ridge, Margaret Thornton (eds), *New Directions for Law in Australia: Essays in Contemporary Law Reform* (ANU Press, 2017) 449, 454.

428 McGinness (n 424) 74-89.

429 Hardy and Williams (n 426) 801-804.

430 Australian Human Rights Commission (AHRC), *Review of Crimes Act 1914 and Other Crimes Legislation of the Commonwealth* (Report No 5, August 1983) 7 [26].

- prejudice the protection of public safety.[431]

The ALRC reiterated these views in its submission to this review.[432] Of the offences in Part 5.6, s 122.2 (discussed in **Chapter 5**) is the closest to the ALRC model. The general offence in s 122.4 is clearly broader than that envisioned by the ALRC.

Introduction of section 122.4

7.8 The enactment of s 122.4 was described as being for 2 primary purposes: first, to adapt to the modern threat environment; and, second, to create a 'narrower and modernised version' of s 70.[433]

7.9 When s 122.4 was enacted, a sunset clause was included to create a 5-year time frame in which the government could review each of the 295 non-disclosure duties attached to the offence and determine whether s 122.4 should be converted into a standalone specific secrecy offence or whether criminal liability was no longer required.[434] That 5-year period ended in December 2023; however, the *Counter-Terrorism and Other Legislation Amendment Act 2023* (Cth), passed in November 2023, extended the sunset date until 29 December 2024.[435]

7.10 AGD's *Review of Secrecy Provisions* identified some issues with s 122.4:

> the Review found some gaps in departments' understanding that non-disclosure duties automatically attract criminal liability under section 122.4 of the Criminal Code, as well as overlap in applying sanctions. For example, some non-disclosure duties attract a criminal penalty as well as administrative or civil sanctions (including those imposed by the APS Code of Conduct).[436]

7.11 It ultimately recommended that s 122.4 in its current form be repealed or allowed to sunset on 29 December 2024.[437] As discussed below, AGD also recommended a new general offence be enacted.

---

431 Australian Law Reform Commission (ALRC), *Secrecy Laws and Open Government in Australia* (Report No 112, December 2009) 23–24 ('*ALRC 2009 Secrecy Laws Report*').

432 ALRC, *Submission 3*, 1–2.

433 Revised Explanatory Memorandum, National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2018 (Cth) 28 [123] ('*EFI Bill*').

434 Attorney-General's Department (AGD), *Review of Secrecy Provisions* (Final Report, 21 November 2023) 40 [174] ('*AGD Review of Secrecy Provisions*').

435 *Counter-Terrorism and Other Legislation Amendment Act 2023* (Cth) s 63.

436 *AGD Review of Secrecy Provisions* (n 434) 41 [175].

437 *AGD Review of Secrecy Provisions* (n 434) recommendation 5.

AGD has proposed a new general offence

7.12 In the AGD *Review of Secrecy Provisions*:

> [AGD identified] that in the majority of cases, the general secrecy offences do not cover the types of information covered by specific secrecy offences and could not be relied upon instead. This includes specific secrecy offences that protect personal information and commercially sensitive information.[438]

7.13 AGD found that departments were 'open to the concept of repealing specific secrecy offences' if the application of general offences were broadened sufficiently. This approach would be consistent with the review's object of consolidation of secrecy offences. It therefore recommended that a new general secrecy offence should be enacted in Part 5.6 to replace s 122.4.[439]

7.14 AGD suggested the definition of 'Commonwealth officer' could be amended to capture all individuals and entities who provide 'services to the Commonwealth'.[440] As discussed in **Chapter 1**, the definition of 'Commonwealth officer' includes contractors, and the inclusion of the phrase '[any person] otherwise engaged to perform work for a Commonwealth entity' in each offence means that the application of the offences is already broad. The definition of 'Commonwealth officer' should not be expanded lightly, particularly as all those who are not Commonwealth officers but are 'otherwise engaged to perform work for a Commonwealth entity' are already covered. As discussed in **Chapter 8**, different criminal thresholds are appropriate for those who do not have a direct relationship with the Commonwealth.

7.15 The key features of the new offence proposed by the AGD *Review of Secrecy Provisions* are that a replacement for s 122.4:

- be informed by the duty not to disclose information that applies to Australian Public Service (APS) employees under reg 7 of the *Public Service Regulations 2023*
- not rely on other laws to impose a duty in the way s 122.4 currently does
- be sufficiently broad to capture all individuals providing services to the Commonwealth, whether paid or not

438 *AGD Review of Secrecy Provisions* (n 434) 34 [141].
439 *AGD Review of Secrecy Provisions* (n 434) 34 [141], recommendations 3 and 4.
440 *AGD Review of Secrecy Provisions* (n 434) 34 [143]. The report refers to an allegation that confidential Commonwealth information disclosed to individuals working at PwC Australia was used to gain financial advantages.

- apply to disclosures that are either:
  - prejudicial to the effective working of government (noting embarrassment would not be sufficient to establish prejudice)
  - of information that was communicated in confidence and disclosure would breach that confidentiality obligation
- be subject to the existing defences in s 122.5, including the defence for public interest journalism
- would not override existing whistleblowing frameworks that allow information to be provided under the PID Act and to integrity bodies, including the National Anti-Corruption Commission (NACC) and the Commonwealth Ombudsman.[441]

7.16 AGD said that the 'existing defence in s 122.5 of the *Criminal Code* should be available for the new general secrecy offence, including the defence for public interest journalism'.[442] It is not clear what role the defence for journalists is intended to have in an offence that applies to Commonwealth officers and others engaged to perform work for a Commonwealth entity, unless there is a proposal to significantly expand the class of people covered by the offence so that it would include journalists working for news media organisations.

7.17 Initial reactions from academics, commentators and civil society groups were critical of the proposed thresholds as 'too low',[443] 'worryingly sweeping'[444] and 'unnecessary and goes too far'.[445] It was also argued that 'greater harm' should be required to invoke criminal liability.[446] There was a consistent view in submissions to this review that any new general offence conform to the principles originally set out in the ALRC 2009 Secrecy Laws Report (see above).[447]

441 *AGD Review of Secrecy Provisions* (n 434) 34–5 [141]–[148].

442 *AGD Review of Secrecy Provisions* (n 434) 35 [149].

443 George Williams, 'Reforms to nation's secrecy laws must go further', *The Australian* (online, 7 December 2023).

444 Peter Greste, 'Australia's secrecy laws include 875 offences. Reforms are welcome, but don't go far enough for press freedom', *The Conversation* (online, 21 November 2023).

445 David Crowe, 'New leadership, same old secrecy', *Sydney Morning Herald* (online, 24 November 2023).

446 Williams (n 443).

447 For example: AHRC, *Submission 17*, [3]–[20]; Mr Philip Boulten SC, Law Council of Australia, *Public hearing transcript*, 26 March 2024, 162; Australia's Right to Know (ARTK), *Supplementary submission 21*, 25–6 [130]; ALRC, *Submission 3*, 12–20; AHRC, *Submission 17*, 4–19 [3]–[73].

Further details of AGD proposal provided

7.18 In their submission to this review, AGD noted that the features of the proposed new offence were still under consideration:

> The department is giving further consideration to the appropriate elements of the offence having regard to the potential for the new offence to replace existing offences and to the kinds of harms that should appropriately be targeted. For example, this could include harms to individuals that can be caused by the improper disclosure of sensitive personal information this is entrusted to government, or harm to the administration of government that can be caused by improper disclosure of confidential information (such as in the PwC example).[448]

7.19 At the public hearing, AGD explained why they consider criminal sanctions are required:

> This information … if disclosed … can still have a very significant impact. And I think the PwC example is just an obvious one of what that enabled. And I think for those of us who are Commonwealth officers and have particular employment obligations, or individuals who provide services and enter into confidentiality obligations where they then have information where it can result in that significant harm. [I]n that case, … quite a significant undermining of … tax policy and [tax] evasion … was enabled.
>
> [T]he idea that disciplinary and administrative sanctions are sufficient is just not the case. … Obviously, … as a public servant where we breach such an obligation, [we] potentially have our employment terminated … But the extent to which that imposes a sufficient penalty obviously varies according to the individual. It may be that has very little impact. And I think the seriousness of what harm a disclosure might cause is worthy in a range of cases of a criminal penalty being possible to apply.[449]

7.20 AGD also suggested that it was considering that the offence might include deemed harm elements, at least for some categories of personal information:

> … something we would like to look at is whether there are some categories, say, of personal information that are so clearly sensitive. Some of those things might be the kind of things that are covered in the sort of sensitive personal information in the Privacy Act, but I don't think that's an entirely neat fit. But things like very sensitive health information, for example, whether it might also be appropriate to cover that improper disclosure of that information by a Commonwealth officer who's entrusted with it without having to then particularly show that disclosing it harmed a person.[450]

7.21 It should be noted that written submissions to this review reflected on s 122.4 in its current form and the offence proposed in the AGD *Review of Secrecy Provisions* – not the

448 AGD, *Submission 7*, 15 [73].
449 Ms Sarah Chidgey, AGD, *Public hearing transcript*, 26 March 2024, 156–7.
450 Ms Sarah Chidgey, AGD, *Public hearing transcript*, 26 March 2024, 154.

developments that AGD discussed at the public hearing, although it is fair to assume that many of the same concerns would still apply.

7.22 The concerns of submitters can be categorised into 3 main themes:

- breadth, proportionality and necessity
- compatibility with art 19 of the ICCPR
- consistency with the implied freedom of political communication.

7.23 I discuss these in turn.

Breadth, proportionality and necessity

7.24 A number of submissions were concerned that the proposed offence was over-broad and disproportionate to any identified harm or threat which is not addressed by other existing offences or civil and administrative penalties. Concerns were particularly centred on the 2 thresholds: where a disclosure is 'prejudicial to the effective working of government' or 'communicated to them in confidence and disclosure would breach a confidentiality obligation'.

7.25 In the ALRC 2009 Secrecy Report, the ALRC expressly said that 'to warrant a criminal penalty, disclosures must harm more than the effective working of government or commercial or personal interests'.[451]

7.26 While the AGD Review of Secrecy Provisions acknowledged this, AGD said it came to a different view because:

> [The] disclosure of information that harms the effective working of government undermines the Australian community's trust in government and the ability of Commonwealth departments and agencies to deliver policies and programs. It is appropriate that conduct which causes or is likely to cause prejudice to the effective working of government be captured.[452]

7.27 However, most submissions to this review on this issue remained supportive of the ALRC's position and said these types of disclosures are better dealt with administratively or through civil remedies.[453] For example, the Law Council of Australia suggested that the threshold that

451 *ALRC 2009 Secrecy Report* (n 431) 274 [8.5].

452 *AGD Review of Secrecy Provisions* (n 434) 35 [146].

453 ARTK, *Supplementary submission 21*, 25–6 [130]; ALRC, *Submission 3*, 12–20; AHRC, *Submission 17*, 4–19 [3]–[73].

AGD proposed was too 'broad and ambiguous [a] concept to import into the criminal law context'. The Law Council supports greater specification of the level of prejudice required.[454]

7.28 In relation to the second test, 'where disclosure was communicated to them in confidence and disclosure would breach a confidential obligation', the Law Council highlighted that the threshold appears to be framed as a deemed harm offence where it is not necessary that the breach occasioned or risked any harm to a public interest. They reiterated their position that general offences should be subject to an express harm element.[455]

7.29 ALRC reiterated to this review

> The role of the criminal law in publicly punishing, deterring, and denouncing offending behaviour is appropriate when applied to behaviour that harms, is reasonably likely to harm or intended to harm essential public interests. Given the adverse consequences of a criminal conviction, however, it is the ALRC's view that it is inappropriate to apply such penalties to disclosures that were not intended and are unlikely to cause such harm.[456]

7.30 AHRC gave similar evidence on the disclosure of sensitive personal or commercial information, saying criminal sanctions should be reserved for unauthorised disclosures that harmed essential public interests.[457]

7.31 The Law Council of Australia also queried whether it was appropriate to tie the proposed offence to the duty not to disclose information under reg 7 of the Public Service Regulations. It highlighted that reg 7 does not apply to several types of government employees – for example, members of the Australian Federal Police, ministers and ministerial staff.[458]

7.32 AHRC considered the proposed threshold was too low:

> The low threshold contemplated by the proposed 'catch all' offence does not strike the right balance between the public interest in open and accountable government and adequate protection for Commonwealth information that should legitimately be kept confidential.[459]

Article 19 of the ICCPR

7.33 AHRC submitted that an offence 'based on such broad thresholds may be inconsistent with the implied right to freedom of expression in art 19 of the ICCPR'.[460] This is an issue, they

454 Law Council of Australia, *Submission 19*, 35 [114].
455 Law Council of Australia, *Submission 19*, 35 [115].
456 ALRC, *Submission 3*; *ALRC 2009 Secrecy Laws Report* (n 431) 118 [4.77].
457 Ms Lorraine Finlay, Human Rights Commissioner, AHRC, *Public hearing transcript*, 25 March 2024, 34.
458 Law Council of Australia, *Submission 19*, 36 [117].
459 AHRC, *Submission 17*, 19 [74].
460 AHRC, *Submission 17*, 18–19.

suggest, that could be ameliorated by strengthening public interest disclosure frameworks outside the *Criminal Code*.[461] At the public hearing, AHRC added that there were a number of alternative legal and administrative mechanisms that could achieve the result of punishment and deterrence without criminalisation. The Commissioner noted, '[t]here are continuing obligations of confidentiality in terms of a variety of mechanisms that may be available' in the case of both current and former Commonwealth officers.[462]

7.34 In the same vein, the Law Council submitted:

> The United Nations Human Rights Committee has emphasised that 'it is not compatible with [Article 19], for instance, to invoke such laws to suppress or withhold from the public information of legitimate public interest that does not harm national security' and that proportionality in such circumstances requires 'establishing a direct and immediate connection between the expression and the threat'. The Law Council considers … that the conviction of an individual under Part 5.6 in cases where the disclosure did not, or was unlikely to, result in serious harm is unlikely to be proportionate under Article 19 of the ICCPR. The absence of a serious harm test for general secrecy offences under Part 5.6 may thus render these offences inconsistent with the protections under the ICCPR.[463]

7.35 While the AGD *Review of Secrecy Provisions* did not expressly discuss these issues, in its submission to this review, AGD did point out that art 19(3) of the ICCPR may be limited as provided by law and when necessary to protect the rights or reputations of others, national security, public order or public health or morals.[464] See **Chapter 3** for further discussion on what sort of limits are permissible.

The implied freedom of political communication

7.36 The joint academic submission did not support AGD's proposed offence because its capacity to 'be interpreted in widely-varying and unpredictable ways' puts its consistency with the constitutional implied freedom of political communication into question. The operation and breadth of the implied freedom is outlined in **Chapter 3**.

7.37 The joint academic submission notes that, since the proposed provision clearly constrains the communication of political matters, a constitutional question arises as to whether the offence has a legitimate purpose and would be a proportionate approach to achieving that purpose. They say that if the legitimate purpose is protecting the 'effective working of government':

> … such a phrase is so vague as to be unclear and potentially unworkable (particularly in the context of a criminal offence). For instance, the 'effective working of government' may

461 AHRC, *Submission 17*, 20.
462 Ms Lorraine Finlay, Human Rights Commissioner, AHRC, *Public hearing transcript*, 25 March 2024, 36.
463 Law Council of Australia, *Submission 19*, 13 [16].
464 AGD, *Submission 7*, 15 [71].

> require efficiency and expediency, or it may call for effectiveness that encompasses democratic accountability and scrutiny. It not only begs questions as to what is 'effective', but what is the 'government'. Does it pertain only to the Executive, including the entire Australian Public Service or, conversely, only upper-level public servants, or even the Ministry. Or, does it encompass Parliament, the justice system and statutory bodies as well? The effective working of any or all of these aspects of 'government' may require different things, so that assessing whether an action compromised 'the effective working of government' becomes an uncertain, highly complex and difficult task.[465]

7.38 Although the offence may be 'rationally connected' to this purpose, the joint academic submission states:

> the protection of all information communicated in confidence, no matter what it's content or the context of that communication, may well go too far and be unnecessary to achieve the purpose, or not 'adequately balanced' (the third step in assessing proportionality).[466]

7.39 Interpreting a broadly drafted reference to the 'workings of government' with deference to the implied freedom in some circumstances, it is possible that a court could find that a disclosure in the public interest actually assisted the efficient working of government by exposing it to the public, giving rise to an implicit public interest defence.

7.40 Alternatively, if the legitimate purpose is one of national security then the joint academic submission suggests that the thresholds set out in the proposed offence arguably go beyond what is necessary to achieve that purpose and be 'rationally connected' to it.[467]

7.41 In its submission, AGD notes that 'any offence that is introduced will be informed by advice on constitutional and international law requirements'.[468]

Provisional findings

7.42 AGD's work on developing a new general secrecy offence has been occurring in parallel with this INSLM review. Some early drafts have been circulated within government, but at the time this report was being finalised no settled position had been reached and AGD's consultation with affected agencies was ongoing. Therefore, my comments in this chapter can only relate to matters of general principle, not to a specific proposed provision.

---

465 Joint Academic Submission, *Submission 13*, 17.

466 Joint Academic Submission, *Submission 13*, 18.

467 Joint Academic Submission, *Submission 13*, 17–18. See Chapter 3 for an explanation of the tests set out by the High Court in relation to the implied freedom of political communication.

468 AGD, *Submission 7*, 15 [70].

7.43 It would be desirable, as the Law Council of Australia has suggested, that consultation extend to non-government groups and include the circulation of an exposure draft.[469] AGD should consider the submissions on the proposed general offence that have been provided to this review.

7.44 My understanding is that AGD is proposing that a new offence is necessary and proportionate on two grounds. First, in order to reduce the overall number of specific secrecy offences and second to address a potential gap highlighted by the alleged 'PWC breach' and its harm on the effective working of government and possibly other 'gaps'.[470] Each of these is discussed further below.

7.45 As detailed in **Chapter 1** of this report, the AGD Review of Secrecy Provisions articulated 12 principles for secrecy offences. The following ones are particularly relevant to a general offence:

- PRINCIPLE 1 – Secrecy offences should be limited to circumstances where there is an essential public interest that requires criminal sanctions.
- PRINCIPLE 4 – A harms-based approach should be taken in framing secrecy offences. Secrecy provisions should:
  - contain an express harm element
  - cover a narrowly defined category of information and the harm to an essential public interest is implicit, or
  - protect against harm to the relationship of trust between individuals and the Government integral to the regulatory functions of government.
- 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.

7.46 These are sound principles and should be at the forefront of the design of any new secrecy offence.

7.47 Most of the provisional findings and recommendations in this chapter are closely related to principles articulated elsewhere in this report – in particular, **Chapters 4** and **5**. Therefore, they should be read together with the rest of this report.

Who should be covered

7.48 As discussed in **Chapter 1**, the combined categories people who are or have been 'Commonwealth officers' and 'other people who undertake work for a Commonwealth entity' is broad. If there is a demonstrated need to extend this to others who have an 'agreement or arrangement' with the Commonwealth care should be taken to ensure that it

469 Law Council of Australia, *Submission 19*, 35 [113].

470 *AGD Review of Secrecy Provisions* (n 434), 35 [144].

is only extended as far as is clearly necessary and that the class of people covered by the 'officials' offences continues to be those with a contract or some relationship of trust or duty with the Commonwealth.

7.49 Offences for people who do not have a contract or relationship of trust with the Commonwealth should continue to be dealt with separately (see **Chapter 8**).

Repeal of other offences

7.50 A primary justification for the proposed new secrecy offence is to enable a reduction in the overall number of specific secrecy offences outside the *Criminal Code*. That is, the new offence would be wide enough to replace a significant number of existing offences, but no wider than necessary to replace those offences.

7.51 Vague comments like 'departments were open to the concept of repealing specific secrecy offences in reliance on new general secrecy offences… [but that] many departments advised that a new general secrecy offences may not necessarily replace the need for specific secrecy offences…'[471] are not, of themselves, a convincing reason for enacting a new law.

7.52 Repeal of identified specific offences should occur at the same time a new offence is enacted to enable the parliament to make a proper assessment as to whether the new offence is necessary and proportionate. That assessment cannot be made if a review is only conducted at the discretion of individual agencies after the new provision is enacted. There is little reason to have confidence that departments and agencies will self-identify offences to be repealed at a later point.[472] Although, if additional offences are identified as redundant later by a subsequent review they should also be repealed.

Harm-based and clear

7.53 The second reason for enacting a new offence is to remedy an actual 'gap' in the criminal law. That is, where there is an identified harm that warrants criminal sanction and is not presently criminalised.

7.54 As noted above, policy work is ongoing. A clear and specific 'gap' has not yet been articulated, but it may arise as a result of the ongoing policy work. The AGD *Review of Secrecy Provisions* refers a couple of potential 'gaps' or harms to which the new offence might be directed. One 'potential gap' is described by AGD as being highlighted by the alleged 'PwC Australia breach'.[473] The facts and circumstances involved with that matter are the subject of other

471 *AGD Review of Secrecy Provisions* (n 434) 34 [141-2].
472 As is proposed by Recommendation 4 of the *AGD Review of Secrecy Provisions* (n 435).
473 *AGD Review of Secrecy Provisions* (n 434) 35 [144].

reviews and were not examined in this INSLM review, so I cannot make any comment on whether this is an actual gap at this point.

7.55 In the AGD *Review of Secrecy Provisions*, the department also describes a possible category of harm to the public interest connected to trust in government:

> Disclosure of information that harms the effective working of government undermines the Australian community's trust in government and the ability of Commonwealth departments and agencies to deliver policies and programs.[474]

7.56 In the consideration of a new secrecy offence designed to improve 'trust', it is worth remembering that a surfeit of secrecy can itself undermine trust in government.

7.57 AGD also mentions 'compromise to the operation of a Commonwealth regulator or new laws or policies' as potential harms that could arise from the disclosure of 'confidential information'.[475] It is not clear if this is intended to be the same 'gap' as the 'PwC Australia breach'.

7.58 As ALRC has articulated, general offences should be harm-based and should relate to essential public interests. The types of essential public interests ALRC articulated (primarily security, defence, international relations and law enforcement) appear to be covered by the other general offences in Part 5.6, including as modified by recommendations in this report.

7.59 Assuming that the ongoing work being done by AGD identifies new 'gaps' and harms to essential public interests, these should be described clearly. Criminal sanctions should only apply to the types of disclosures that genuinely cannot be adequately dealt with by existing contractual and administrative remedies.

7.60 The new offence should be harms-based. If there is some sound reason that a part of the offence (or a separate offence) needs to be a deemed harm offence then any deemed harm element should be limited to a very narrow category of information the disclosure of which will always, or almost always, result in a significant harm to an essential public interest.

Law enforcement

7.61 As discussed in **Chapters 4** and **5**, a cascading approach should be taken to penalising disclosures that interfere with the criminal justice system. For the reasons already articulated in those chapters, the general offence should contain a provision, consistent with the original ALRC recommendation, to penalise disclosures that would prejudice the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth. This should apply regardless of the agency involved.

---

474 *AGD Review of Secrecy Provisions* (n 434) 35 [146].

475 *AGD Review of Secrecy Provisions* (n 434) 35 [148].

Penalty

7.62 The offences in s 122.1 and 122.2 as modified by the recommendations of this review will deal with disclosures by officials and others performing work for the Commonwealth that could a have serious impact on essential public interests connected to security, defence, international relations and the capabilities of intelligence agencies and the use of statutory powers by law enforcement agencies as well as harm to the health or safety of the Australian public. It is appropriate that these kinds of harm carry the serious 7–10-year penalty. From what has been articulated to date about the proposed new offence, there is no reason to think that a penalty higher than the existing 2-year penalty will be necessary to deter or punish the kind of conduct contemplated.

Recommendation

RECOMMENDATION 11: Any general offence to replace s 122.4 should be consistent with the following principles:

- **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.**
- **The offence should be harm-based and relate to essential public interests. However, if 'deemed harm' offences are to be incorporated, they should be limited to a very narrow category of information where significant harm to an essential public interest is always, or almost always, going to be the result.**
- **The offence should cover only disclosures that cannot be adequately dealt with by existing remedies including contractual and administrative remedies.**
- **Broad and uncertain language such as 'functioning of government' should be avoided.**
- **The offence should apply to current and former Commonwealth officials and others who perform work for a Commonwealth entity in relation to information acquired in the course of their duties. However, if the scope of the offence is to be broadened it should still be closely linked to some kind of contract, agreement or arrangement with the Commonwealth.**
- **The penalty for reckless conduct should be no more than 2 years imprisonment.**

7.63 If a primary justification for the new general offence is to replace specific existing offences then the offences to be repealed should be included in the legislative proposal in order to allow the parliament to properly assess the necessity and proportionality of the proposed new offence.

7.64 It is desirable that a consultation draft of the bill creating any new general offence be circulated, including to non-government organisations.

Chapter 8: Offence for non-officials

8.1 Most of the offences in Part 5.6 of the *Criminal Code* apply only to current and former Commonwealth officers and other people engaged to perform work for a Commonwealth entity (see **Chapter 1**).[476] This reflects the fact that it is those people that the Commonwealth must directly entrust with sensitive information in order to operate. People who choose to work for government as employees, contractors or otherwise, including in sensitive areas like intelligence and law enforcement, voluntarily take on those responsibilities and are usually remunerated by the Commonwealth for doing so. Breach of that trust between the Commonwealth and those engaged to serve it brings a level of criminal culpability and warrants criminal sanctions to deter and punish improper disclosure by Commonwealth employees and contractors.

8.2 In contrast, the offences in s 122.4A apply to non-officials – that is, people who do not have any direct relationship with the State and are not directly employed or otherwise engaged to handle government information. This category includes people such as journalists whose role in a democracy includes directly critiquing the work of government and seeking to enable citizens to understand and make choices about who they want to govern them. Nevertheless, non-officials will occasionally come into possession of the type of sensitive government information that, in the wrong hands, could harm Australia's national interests.

8.3 For the reasons given in **Chapter 6** I have recommended that 'dealing with' offences for non-officials should be removed (**Recommendation 8**).

8.4 As noted in **Chapter 1**, there is a possible anomaly in relation to ABC and SBS staff and contractors, who are expressly excluded from the definition of 'Commonwealth officer' but may nevertheless be 'otherwise engaged to perform work for a Commonwealth entity' because ABC and SBS are both Commonwealth entities. As a result, ABC and SBS staff and contractors may not be covered by the non-officials offence in s 122.4A and instead be covered by the offences in ss 122.1, 122.2 and 122.4. As I have suggested in **Chapter 1**, this outcome is likely to be unintentional and could easily be remedied via the making of a regulation (or through legislative amendment).

476 The offences for officials are the deemed harm offence in s 122.1 (Chapter 4); the serious harm-based offence in s 122.2 (Chapter 5); aggravated offences (Chapter 6); and, the general offence (Chapter 7). There are similar offences in other Acts, some of which such as those in the *Intelligence Services Act 2001* (Cth), the *Office of National Intelligence Act 2018* (Cth) and the *Australian Security Intelligence Organisation Act 1979* (Cth) ('*ASIO Act*'). As discussed in Chapter 6, there are presently 'dealing with' offences for both officials and non-officials, although Recommendation 8 proposes that these should apply only to officials.

8.5 This chapter begins by examining the question of when and in what form offences for non-officials are appropriate. This includes briefly summarising what previous reviews have said on the subject, considering international comparisons and submissions to this review. It concludes that offences for non-officials who disclose certain information can be appropriate, but they need to be harm-based and have a higher threshold than offences for officials. Offences also need to be clear and certain. The chapter then compares the current offence to these tests. I conclude that some legislative changes are needed.

8.6 It should be noted that there are a number of administrative safeguards, including some specific to journalists, that interact with the way the offences in Part 5.6 currently operate in practice. These are discussed in the safeguards chapter (**Chapter 10**).

8.7 Penalties are discussed at the end of the chapter.

When and in what form might offences for non-officials be appropriate?

Previous reviews

8.8 Previous reviews have considered the appropriateness of secrecy offences for non-officials (**Annex B**). The Australian Law Reform Commission (ALRC) and other independent reviews have consistently recommended that offences for non-officials should have an express harm element.[477]

8.9 Former INSLM the Hon. Roger Gyles AO KC neatly summarised previous reports in the context of his 2015 review of a secrecy provision in s 35P of the *Australian Security Intelligence Organisation Act 1979* (Cth) (*ASIO Act*). In highlighting one of the 3 basic flaws of s 35P – the absence of an express harm requirement for breach by a journalist or other third party[478] – he said:

> The fundamental question is whether third parties should be bound by the broad prohibitions of external disclosures effected by section 35P in the same way as insiders … The section makes no distinction, either in culpability or penalty. There is no 'harm' requirement in the basic offence. That is contrary to the reasoned position of the ALRC, the Gibbs Committee and the Commission of Inquiry into ASIS. For example, the Gibbs Committee recommended that, in the case of a disclosure relating to the intelligence and security services, the

477 See, eg, Australian Law Reform Commission (ALRC), *Secrecy Laws and Open Government in Australia* (Report No 112, December 2009) 191 [6.29] ('*ALRC 2009 Secrecy Laws Report*').

478 *ALRC 2009 Secrecy Laws Report* (n 477) 23 [44].

> prosecution would not have to prove damage, but would have to prove damage if the disclosure was made by a person who was not a member or ex-member of those services.[479]

8.10 Mr Gyles recommended that additional harm elements should be required to be proven for the third-party offences. This recommendation was implemented.[480]

8.11 The ALRC recommended that subsequent disclosure offences for non-officials be limited to circumstances where the non-official knows, intends or is reckless as to whether their disclosure will harm – or knows or is reckless as to whether their disclosure is reasonably likely to harm – one of the essential public interests that the ALRC described.[481]

8.12 The recent Attorney-General's Department (AGD) *Review of Secrecy Provisions* said that 'offences capturing third parties should have a higher threshold for establishing criminal liability'.[482] However, that review also said that it considered the current offences in s 122.4A already have a higher threshold for establishing criminal liability because:

> they apply to narrower categories of harm than the general secrecy offences applying to Commonwealth officers, and apply the fault element of recklessness (the person is aware of a substantial risk that a circumstance does or will exist, and having regard to this it is unjustifiable to take the risk).[483]

8.13 As currently drafted, the offence for non-officials applies to one of the 3 current categories of 'inherently harmful information' and 3 of the 5 current categories of information that 'cause harm to Australia's interests' (see **Chapters 4** and **5** for a discussion of those defined terms). With the exception of security classified information, each of the categories of information for non-officials clearly requires proof of some kind of damage, harm or prejudice to a public interest. The fault (mental) element for non-officials is the same as it is for officials: recklessness.

8.14 Although it may be accepted that the offences for non-officials apply to a subset of the categories of information covered by ss 122.1 and 122.2, this is not the same as applying a higher threshold for establishing criminal liability. A better example of a higher threshold is an additional element, such as a requirement that actual harm be established rather than

---

479 Roger Gyles, INSLM (former), *Report on the impact on journalists of section 35P of the ASIO Act* (Report, October 2015) 22 [42] ('*INSLM Section 35P Report*').

480 *INSLM Section 35P Report* (n 479) 24–5. This recommendation was implemented by amendments to the *ASIO Act* in sch 18 of the *Counter-Terrorism Legislation Amendment Act (No. 1) 2016* (Cth).

481 *ALRC 2009 Secrecy Laws Report* (n 477) recommendation 6–6.

482 See Attorney-General's Department (AGD), *Review of Secrecy Provisions* (Final Report, 21 November 2023) 24–5, principle 7 ('*AGD Review of Secrecy Provisions*').

483 *AGD Review of Secrecy Provisions* (n 482) 42 [185].

deemed harm or that the fault (mental) element be raised from recklessness to knowledge or intention.

Equivalent offences in Five Eyes countries

8.15 In other Five Eyes countries where offences for non-officials exist, they require not only harm but also an intention or knowledge that the harm will occur or at least a reasonable belief harm will occur.[484] They are also generally subject to lower penalties.

8.16 The United Kingdom has a general offence under s 5 of the *Official Secrets Act 1989* (UK) which applies to non-officials. It penalises unauthorised disclosures of information protected by the other offences in that Act (broadly, intelligence, defence, international relations, law enforcement, foreign confidences and special investigation powers) where the disclosure is damaging *and* the person makes the disclosure knowing, or having reasonable cause to believe, that it would be damaging.[485] A person who commits this offence is liable to a maximum sentence of 2-years imprisonment.[486] A recent UK review by the UK Law Commission recommended that harm remain an essential feature of offences for non-officials.[487]

8.17 Canada has an offence in its statute book that is broadly similar to the former s 79 of the *Crimes Act 1914* (Cth).[488] The offence applies to any person who possesses or controls any secret official information (particularly in relation to defence) and:

- communicates this information to any person (unless authorised or it is in the interest of the State)
- uses the information for the benefit of a foreign power or in any other manner prejudicial to the safety or interests of the State
- retains the information contrary to their duty or failure to comply with any directions to return or dispose of the information, or
- fails to take reasonable care of this information.

---

484 The term 'Five Eyes' refers to the intelligence sharing relationship between the United States of America, the United Kingdom, Canada and New Zealand in addition to Australia.

485 *Official Secrets Act 1989* (UK) s 5(3).

486 *Official Secrets Act 1989* (UK) s 10.

487 Law Commission (UK), *Protection of Official Data* (Report No 395, 1 September 2020) 66 [4.43] ('*UK Protection of Official Data Report*'). That review also recommended that the 2-year maximum sentence (which currently applies to officials and non-officials alike) be reviewed, noting that there is a 'cogent argument for saying that primary disclosures and secondary disclosures should not be equated for the purposes of maximum sentence'; 89 [5.68].

488 *Security of Information Act*, RSC 1985, c O-5, s 4(1) (Canada).

There appears to be no distinction in maximum penalty for the primary offences in the Act (which also includes foreign interference and terrorism-related communication offences) with the penalty being up to 14 years imprisonment.[489] However, the offence provision that applies to non-officials (summarised above) was found to be invalid in 2006, as it was contrary to the *Canadian Charter of Rights and Freedoms*.[490]

8.18 New Zealand has 2 offences that apply to non-officials. Under s 78A of the *Crimes Act 1961* (NZ), it is offence for anyone who 'owes allegiance to the Sovereign in the Right of New Zealand' to:

- knowingly communicate official information knowing that communication is likely to prejudice the security or defence of New Zealand, or
- retain any official document with the intent to prejudice the security or defence of New Zealand, or
- knowingly fail to comply with any lawful direction for the return of an official document which would be likely to prejudice seriously the security or defence of New Zealand if disclosed.[491]

A person who commits an offence under this section is liable for imprisonment for a term not exceeding 3 years. In addition, there is a summary offence (maximum penalty 3 months imprisonment or a fine of $2,000) under s 20A of the *Summary Offences Act 1981* (NZ) for any person who communicates 'official information' knowing that doing so is likely to result in one or more of the harms listed in that offence.[492]

8.19 No directly equivalent provision was identified in United States law. The US does have espionage laws that apply to any person. They are broadly similar to the espionage offences under Part 5.2 of the *Criminal Code*.[493] There is also an offence that is in some ways similar to the foreign interference offences in Part 5.2.[494]

489 *Security of Information Act*, RSC 1985, c O-5, s 27.

490 *Security of Information Act*, RSC 1985, c O-5, s 4. See also *O'Neill v Canada*, in which ss 4(1)(a), (3) and (4)(b) of the *Security of Information Act* were found to be invalid as contrary to s 2(b) (freedom of expression and the press) and s 7 (principles of fundamental justice) of the *Canadian Charter of Rights and Freedoms*, and could not be saved by s 1 as a reasonable limit imposed by law in a free and democratic society: *O'Neill v Canada (Attorney General)* [2006] OJ 4189, [5]–[7], [65], [72], [80]–[84], [103]–[105].

491 *Crimes Act 1961* (NZ) s 78A.

492 *Summary Offences Act 1981* (NZ) s 20A.

493 18 USC § 793, 794, 795, 797 and 798.

494 18 USC § 798.

Submissions on the application of a secrecy offence to non-officials

8.20 I received a range of submissions from civil society and government organisations on the offence for non-officials. Submissions that go to the general idea of when a criminal offence is appropriate for non-officials and compliance with Australia's international obligations in relation to freedom of communication are summarised here. Later in this chapter submissions specific to individual parts of the current offence are discussed.

Differentiating between the 'duty' of officials and others

8.21 There was broad agreement among all of the submitters who addressed the issue that officials and non-officials should be treated differently. The Law Council of Australia said that it was appropriate to differentiate between offences for Commonwealth officers and contractors and others:

> The Law Council agrees with the weight of reasoning across multiple reviews supporting the differentiated treatment of 'insiders', that is, Commonwealth officers or contractors who are entrusted with sensitive information in the course of their duties and, therefore, owe a special duty to maintain confidentiality. Among Commonwealth officers, as identified by the Gibbs Committee, members of intelligence and security services are in a position of particular trust and are rightly subjected to greater restrictions in relation to Commonwealth information than other Commonwealth officials and outsiders.[495]

8.22 The Australian Secret Intelligence Service (ASIS) similarly noted the need for there to be a distinction between Commonwealth officers and other entrusted persons and non-Commonwealth officers:

> There should be a distinction between 'Commonwealth officers and other entrusted persons' and 'non-Commonwealth' officers in regards to secrecy offences. Entrusted persons should be held to a higher standard than the general population.[496]

8.23 The Australian Human Rights Commission (AHRC) submitted that the requirement that disclosures should only be prohibited where they will result in some specific, identifiable harm reflects the principle that limitations on the right to freedom of expression are only justified when they are necessary to achieve a legitimate purpose. AHRC noted that this is of particular importance to disclosures by outsiders, including journalists and whistleblowers.[497]

---

495 Law Council of Australia, *Submission 19*, 16 [31].

496 Australian Secret Intelligence Service, *Submission 10*, 9 [45].

497 Australian Human Rights Commission (AHRC), *Submission 17*, 12 [40]–[42].

8.24 The AHRC also noted that careful consideration of compliance with Australia's international law obligations, particularly the *International Covenant on Civil and Political Rights*, is needed for any offence directed at non-officials. This is because non-officials have no formal relationship with the Commonwealth and no duty of confidence.[498]

8.25 The Law Council of Australia agreed with the AHRC that the current approach to criminalisation of acts by non-officials may be inconsistent with international obligations because it is disproportionate:

> The over-broad approach to criminalisation of a wide range of conduct, in particular, the conduct of civil society actors, such as academics and journalists, risks imposing disproportionate limitations on the right to freedom of expression. The absence of harms-based approach and the deviation from orthodox approaches to identifying culpability increases the risk that limitations will be found to be disproportionate.[499]

8.26 The Human Rights Law Centre (HRLC) said that secrecy offences applying to third-party, non-Commonwealth officers should be repealed. Alternatively, communicative secrecy offences should only apply to non-Commonwealth officers in extremely narrow circumstances, and 'dealing with' offences should have no application to non-Commonwealth officers.[500]

8.27 Australia's Right to Know (ARTK) said that it was inappropriate to impose obligations on a person who has not agreed to be bound:

> There is no justification for imposing a criminal penalty on an 'outsider' to government for failing to adhere to a particular policy of government. In the absence of some further voluntary act – the acceptance of Commonwealth employment, the signing of documents agreeing to be bound by the applicable policy framework, or so on – there is no public policy justification for imposing a criminalised duty on outsiders to adhere to internal policy requirements.[501]

8.28 ARTK's submission states that it 'has been a longstanding view of ARTK, that journalists and those working with them should not be exposed to criminal liability'.[502]

8.29 The Alliance for Journalists' Freedom (AJF) noted that there were legitimate reasons for confidentiality, discretion and absolute secrecy in some circumstances to provide for security services to undertake their work. However, the restrictions on the types of information that can be shared by journalists under the current s 122.4A are 'unnecessarily and disproportionately broad'.[503]

---

498 AHRC, *Submission 17*, 17 [61].
499 Law Council of Australia, *Submission 19*, 10 [4].
500 Human Rights Law Centre (HRLC), *Submission 14*, 9.
501 Australia's Right to Know (ARTK), *Supplementary submission 21*, 2 [6].
502 ARTK, *Submission 12*, 1-2 [2]–[4].
503 Alliance for Journalists' Freedom (AJF), *Submission 11*, [1.11].

8.30 AJF also said that there were certain situations where it was in the public interest to report on matters currently prohibited by s 122.4A, including where no actual harm arises:

> Alternatively, consider a situation in which a journalist publishes leaked information that reveals that political leaders are misrepresenting the conclusions of intelligence assessments conducted by security agencies, in such a way that causes unreasonable fear among voters. Or a situation in which a journalist publishes leaked information that reveals corrupt spending on the part of security agencies. In these scenarios, the information being shared could raise matters in the public interest, such as the conduct of political leaders or government expenditure. Communicating the information has no actual harm or effect, other than to hold the relevant security agency or political leader to account in the interest of transparent and open government. It is neither necessary nor proportionate to subject a journalist or their sources to criminal sanction in such situations.[504]

8.31 HRLC noted that the impact of the current provisions extends beyond journalists and impacts its ability to give legal advice:

> The third party offences in the Criminal Code have posed serious, ongoing concerns for us in the operation of our legal services to clients. The imposition of potential liability in these circumstances is not necessary or proportionate and the law should be amended to remove or significantly reduce application to lawyers and other third parties who are not actively soliciting receipt.[505]

8.32 Mr Philip Boulten SC, member of the National Criminal Law Committee of the Law Council of Australia, made the following comments at the public hearing:

> At a time of heightened risk of foreign interference, the need to strengthen civil society information security may be a legitimate objective. However, ill-defined criminal offences are not an effective or necessary means of achieving that objective. The Law Council is particularly concerned that catch all offences that apply to the conduct of civil society actors, like journalists, risk criminalising a wide range of conduct, including the mere receipt of security-classified information.[506]

Describing the level of harm

8.33 Consistent with previous reviews, I agree that offences for non-officials should be harm-based and have a higher threshold for establishing criminal liability than offences for officials.

8.34 At the moment the harm-based parts of the offence for non-officials use a mixture of terms. One refers to 'damage' (to the security or defence of Australia), another to 'interfere with or prejudice' (the prevention (etc.) of a criminal offence against a law of the Commonwealth) and another to 'harm or prejudice' (to the health or safety of the Australian public). As discussed in **Chapter 5**, the 'or' in the latter 2 phrases appears to be disjunctive, and

504 AJF, *Submission 11*, [3.9].
505 HRLC, *Submission 14*, 8.
506 Mr Philip Boulten SC, Law Council of Australia, *Public hearing transcript*, 26 March 2024, 163.

parliament has presumably intentionally used different words in different paragraphs. In other words, 'interfere', 'prejudice' and 'harm' each potentially have a different meaning. What is more, on its ordinary meaning 'interfere' could be a low bar and may include things such as causing minor delay or inconvenience – neither of which should attract criminal liability for non-officials (see further discussion of these terms in **Chapter 5**).

8.35 While it is ultimately a matter for drafters, the harm element for non-officials should be drafted in a way that makes clear that actual substantive harm is required. In addition, as discussed in this chapter, the offence should remain narrowly focused on serious harms to essential national interests.

Recklessness versus intent or knowledge as the harm element

8.36 Another area of considerable debate is whether the fault (mental) element for non-officials should remain at recklessness or be increased to knowledge or intent. Another option may be for different fault elements to apply to different parts of the offence or for there to be different penalties, as is the case with some other offences, including secrecy offences (see s 35P of the *ASIO Act*.

8.37 The Law Council of Australia said:

> the mental requirement should be intention or knowledge with respect to the physical elements listed in s 122.4A(1)(i)–(iv). If the mental requirement is recklessness, then it should be punishable by a maximum penalty of 12 months.[507]

8.38 HRLC preferred raising the threshold to intent to cause harm:

> [The offence is] … extremely wide. While its effect is somewhat mitigated by the available defences, its scope goes beyond what is justifiable to impose on 'outsiders'. We would recommend that the provision be recast to require intent as to the harm caused by the communication, and those categories of harm be narrowed.[508]

8.39 Several other groups supported this approach:

- The Media, Entertainment and Arts Alliance said that 'agencies should be required to provide proof of intent or the likelihood of harm'.[509]
- ARTK considered that 'any criminal sanction must require an intention to cause harm to a recognisable public interest'.[510]

---

507 Law Council of Australia, *Submission 19*, 27, recommendation 8.
508 HRLC, *Submission 14*, 12–13
509 Media, Entertainment and Arts Alliance (MEAA), *Supplementary submission 22*, 4.
510 ARTK, *Submission 12*, 2.

- The joint academic submission said that the 'dealing with' offence under s 122.4A(2) should not capture mere receipt of security classified information by a non-Commonwealth officer 'unless that information is received intentionally and with knowledge that the information if disclosed would cause harm to national security'.[511]
- AJF endorsed the UK approach of requiring knowledge or reasonable cause to believe that harm would arise.[512]

8.40 In contrast, ALRC recommended recklessness as the fault (mental) element. Government agencies did not make specific submissions on this issue, but I consider it very likely, based on their other submissions, that they would argue that recklessness remains appropriate.

8.41 I have found the issue of what fault (mental) element should apply to secrecy offences for non-officials to be one of the more difficult questions of this review. The arguments for having a higher fault element for non-officials are strong. Equally, the kinds of harm to the national interest that can come from disclosing the narrow category of information that I propose be covered by the offence for non-officials is serious and, unlike 'dealing with' offences, the harm is not contingent on some third party subsequently committing another offence. Recklessness as to harm caused by a disclosure means that the person must be aware there is a substantial risk that the harm will occur and, having regard to the circumstances known to them, it is unjustifiable to take the risk.[513]

8.42 In the end I am recommending that recklessness remain the fault element for disclosure offences for non-officials but that the penalties be adjusted to differentiate between conduct that is reckless as to harm and conduct that a person knows or intends will result in harm. Consistent with **Recommendation 1**, security classification should not be used as an element of the offence in s 122.4A. If that recommendation is not accepted than 'intention to cause harm' or 'knowledge of likely harm' should be the fault (mental) element for that part of the offence. For the reasons given in **Chapter 6** I have recommended that 'dealing with' offences for non-officials should be removed (**Recommendation 8**). If that recommendation is not accepted then intention or knowledge would be the appropriate fault (mental) element for 'dealing with' offences by non-officials if they are to be retained.

511 Joint Academic Submission, *Submission 13*, 3.
512 AJF, *Submission 11*, [3.10].
513 'Recklessness' is defined in s 5.4 of the *Criminal Code Act 1995* (Cth) ('*Criminal Code*') and is also discussed in Chapter 4.

Ancillary offences

8.43 ARTK raised a concern that journalists may be prosecuted under more serious offences of Part 5.6 because they may be taken to assist in the commission of an offence by a Commonwealth officer:

> a journalist may be taken to be a person who 'aids, abets, counsels or procures' the commission of an offence by an 'insider.' This is because the very act of receiving information from a government source is likely to result in a source contravening any of sections 122.1, 122.2, 122.3 or 122.4. The journalist will accordingly be taken to have committed the insider offence and be punished accordingly, provided certain intention and other requirements for accessorial liability are met.[514]

8.44 Ancillary offences apply by default to all offences against laws of the Commonwealth because of Part 2.4 of the *Criminal Code*. Ancillary offences include joint commission, incitement and conspiracy. However, merely receiving information from an official is not sufficient to make the receiver guilty of any of these ancillary offences. Each of the ancillary offences requires active steps be taken by the second person (in this example the journalist) and an agreement or intention that the offence be committed. Also, depending on the ancillary offence, it may also involve additional elements.

8.45 There is no reason to remove or alter the ordinary operation of Part 2.4 of the *Criminal Code*.

General principles for offences for non-officials

8.46 At this point it is useful to summarise my findings on some general principles for secrecy offences for non-officials so that the application of these principles can be considered against the existing offences in the next section. Penalties are dealt with separately at the end of the chapter.

8.47 As with the current s 122.4A, it is not necessary or appropriate for the offence for non-officials to seek to cover all of the same types of information that it is an offence for officials to communicate. The offence for non-officials should continue to be considerably narrower than offences for officials.

8.48 Secrecy offences for non-officials should:

- relate to the communication of information, not 'dealing with' (**Recommendation 8**)
- have an actual harm element and not rely on deemed harm
- apply only to serious harms to the national interest
- continue to be narrower than offences for officials.

514 ARTK, *Submission 12*, 21 [111].

8.49 General principles, including that the law should be clear and knowable and that it be constitutional and compliant with international obligations, also apply. Ancillary offences (such as aiding, abetting, inciting and conspiracy) should continue to apply in the normal way.

8.50 As discussed at the end of this chapter there is scope for differentiation in penalty between conduct that is reckless and conduct done with intent or knowledge of harm.

8.51 For the reasons discussed in **Chapter 9**, I have not recommended the inclusion of a general 'public interest' element in secrecy offences; however, the available defences need to recognise the role of public interest journalism in a democracy.

Analysis of the current offence of disclosure by non-officials

8.52 Having set out some general principles, the remainder of this chapter considers the specific elements of the current disclosure offence for non-officials. The key part of the current offences for non-officials is that one or more of the following must apply:

(i) the information has a security classification of secret or top secret
(ii) the communication of the information damages the security or defence of Australia
(iii) the communication of the information interferes with or prejudices the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth
(iv) the communication of the information harms or prejudices the health or safety of the Australian public or a section of the Australian public.

The fault element is currently recklessness as to whether one of these circumstances applies, and the penalty is up to 5 years imprisonment. As discussed in **Chapter 4**, strict liability currently applies to a security classification being applied in accordance with the policy framework.

8.53 Each of these is considered in turn below.

Security classification as an element of the offence

8.54 **Chapter 4** already explains in detail why it is problematic to rely on security classification as an element of an offence.[515] **Recommendation 1** proposes removing security classification as an element of any of the offences in Part 5.6, including the offence for non-officials.

8.55 Submissions from non-government organisations were particularly strong in their opposition to reliance on security classification in offences for non-officials. It is worth recording some

515 Chapter 4 also briefly discussed the effect of the slightly different terminology used to describe security classification in s 122.4A compared to s 121.1.

of the concerns of non-government groups about the effect of reliance on security classification for non-officials.

8.56 The joint academic submission noted that the designation of a security classification may apply to information that may not necessarily cause harm if disclosed:

> the information may be incorrectly classified for example, or contains information that is classified but may not necessarily contain damaging information, or the source or journalist may have taken steps to redact damaging information, while revealing stories in the public interest.[516]

8.57 ARTK was concerned about a number of issues, including administrative decisions made by officials effectively determining when an offence occurs:

> There is no principled reason to say that an average Australian, under threat of 5 years' imprisonment, must adhere not just to the internal policies of the Commonwealth concerning the confidentiality of its own records (which can change radically from time to time), but must adhere also to any and all 'decisions' of anonymous public servants who apply those policies to any given document when giving it a classification. That is particularly so given that current policy extends to the protection of purely commercial information, and that any 'decision' to affix the stamp may have been factually wrong, may have misinterpreted the policy, may have been motivated by an improper purpose, or may have been correct when made but is no longer appropriate given changed circumstances. Nothing in these circumstances suggests criminal culpability for any 'outsider' in failing to comply with the Commonwealth's policy framework for securing its own documents.[517]

8.58 AJF also queried how historical information would be treated:

> in circumstances where a journalist obtains access to information that they wish to share in the public interest that has been classified according to a policy framework that predates, and has different requirements to, the PSPF. A document created in 2005 would not yet be declassified according to the *Archives Act*, but may have been classified according to a different standard than the PSPF. This causes a practical problem as to what policy would be applied in any prosecution under section 122.4A.[518]

8.59 AJF also pointed to the conclusions of the Law Council of Australia on rule of law issues around deemed harm (which comprises security classification):

> it is a key principle of the rule of law that the law must be readily known, available, certain, and clear. The rule of law requires that laws be public and available so that individuals can be aware of the law prior to their being held responsible for complying with it. The reason for this requirement is that the law is supposed to guide conduct, which it cannot do if it is secret or retroactive. As it stands, the policy framework that is to be applied in a prosecution under section 122.4A is unclear.[519]

---

516 Joint Academic Submission, *Submission 13*, 13.
517 ARTK, *Submission 12*, 24 [125].
518 AJF, *Submission 11*, [4.9].
519 AJF, *Submission 11*, [4.10].

8.60 The uncertainty in knowing whether information is in fact 'security classified information' was raised several times. In this context it is important to note that, as discussed in **Chapter 4**, information must be classified 'in accordance with' the relevant policy framework. Merely having a marking on a document is not enough – that marking must be properly applied under the framework and the decision to apply a classification must be under a policy framework that is consistent with the descriptors of harm in s 90.5(1)(a). In seeking to assess if information is 'classified in accordance with' the relevant policy framework, non-officials may not have access to all of the documents that form part of that policy framework. As Dr Dominique Dalla-Pozza said:

> If the most hard-edged powers of the State in their use of the criminal law can be determined in important instances by a policy document then that makes it very hard for individuals and civil society to know with certainty where the ambit of the criminal law lies.[520]

8.61 Furthermore 'information' may also often come to a journalist, lawyer or civil society group, at least initially, orally and not in the form of a document – making it even more difficult for them to ascertain if it has been 'classified in accordance with' a policy framework.[521]

8.62 The arguments for removing reliance on security classification is even stronger for non-officials than it is for officials. There is no reason that a non-official should be taken to know what a security classification means. Unlike officials, they will not necessarily have knowledge of the 'policy framework', have been trained in how the framework operates or, indeed, even have access to all of it. The rule of law concerns about the use of a policy document, and the uncertainty associated with the use of security markings discussed in **Chapter 4**, are even stronger for a non-official who has no relationship with the Commonwealth.

8.63 Further, reliance on a security classification is a form of deemed harm offence. Secrecy offences for non-officials should have an express harm element and not rely on deemed harm.

8.64 Having recommended removal of 'security classification' from the offence for non-officials, I considered whether another element of the category defined as 'inherently harmful information' should be added to the offence. In particular, I considered whether intelligence information (etc.) of a type contemplated by **Recommendation 2** should be added. In the end I have not recommended this for 2 reasons: first, it may be very difficult for a non-official to identify when information is in that category; and, second, if they do recognise it as being in that category then the offence of recklessly causing serious harm to security or defence that I have recommended retaining (see below) will probably apply. There are also specific

520 Dr Dominique Dalla-Pozza, Australian National University, *Public hearing transcript*, 26 March 2024, 42.

521 See, for example, MEAA, *Submission 9*, 5; HRLC, *Submission 14*, 13.

offences if the information is about the identity of an ASIS or Australian Security Intelligence Organisation (ASIO) staff member or agent.

8.65 As noted in **Chapter 4**, even if 'security classification' as an element of the offence is removed, markings on a document may still be relevant to proving as a matter of fact that a person was reckless (or had knowledge or intention) in relation to the harm that their disclosure may cause. This will be more difficult to establish for non-officials, who are not trained in classification markings in the way some officials are, but may still be relevant depending on the facts of the case (see the discussion on recklessness in **Chapter 4**).

Information that damages security or defence

8.66 The remaining parts of the offence are harm-based. The first of these is that communication of the information 'damages the security or defence of Australia'.

8.67 Currently the expression 'security or defence of Australia' is defined as:

> ***Security or defence of Australia*** includes the operations, capabilities or technologies of, or methods or sources used by, domestic intelligence agencies or foreign intelligence agencies.

8.68 There was some concern in submissions that this expression vague and uncertain. These are legitimate concerns and are discussed in **Chapter 5**. This can be at least partly addressed by **Recommendation 6** that 'security' be defined by reference to its meaning in the *ASIO Act* and that 'defence' be defined having regard to the recommendations of the former INSLM's review of the operation and effectiveness of the *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth). By using these newly defined terms instead of the current definition, the offence will be more certain and the types of harm contemplated much clearer.

8.69 The offence does not currently refer to international relations (in contrast to the serious harm offence for officials). No submissions proposed changing this.[522] I note that where damage to international relations would also harm security or defence as defined, then that conduct will be covered.

8.70 This element requires actual 'damage' to the security or defence of Australia. Another way of describing this may be 'serious harm'. My intention is that this be a higher threshold than the offence for officials, which, in accordance with **Recommendation 6**, will become 'harm or likely harm' to security or defence.

---

522 The UK Law Commission considered a similar issue in their detailed review of UK secrecy laws and concluded that the categories of information protected by the *Official Secrets Act* (UK) should not be expanded to include economic information in so far as it relates to national security. See *UK Protection of Official Data Report* (n 487) 118 [5.203]–[5.205].

8.71 Examples of disclosures in this category of offence for non-officials might include the targets of a current covert counterterrorism or counter-espionage operation (terrorism and espionage are both within the definition of 'security') or information about the detail of how Australia's 'cyber-warfare' capabilities operate.

Law enforcement-related information

8.72 The third category in the current offence is:

> the communication of the information interferes with or prejudices the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth;

8.73 As discussed in **Chapters 4** and **5**, a cascading approach should be taken to penalising communication and dealing with law enforcement related information by officials. With the changes proposed by **Recommendations 3** and **6**, the higher category offences for officials in relation to law enforcement matters will relate to:

- The technologies, capabilities and methods used to exercise special electronic surveillance powers under warrants – which will be covered by the deemed harm offence for officials (**Recommendation 3**), and
- Harm or likely harm to the utility of operational and technical capabilities and methods connected to special powers granted to any agency to access information or to search people, places or things (other than electronic surveillance) to combat crime – which will be covered by the actual harm offence for officials (**Recommendation 6**).

8.74 With the changes proposes by **Recommendation 11**, the general offence for officials will apply to information that 'impedes the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth'.

8.75 A cascading approach should also be taken to penalising communication of law enforcement related information by non-officials. In the case of non-officials, where there is only one offence, and to maintain differentiation between officials and non-officials, this means setting a higher threshold of harm. As discussed later in this chapter, differential penalties are also recommended.

8.76 Information about electronic surveillance capabilities is a confined category of information and one where it is relatively easy, even for a non-official, to identify whether the information in question is about that type of capability. When it comes to undermining the utility of the technology, capabilities and methods that are used to support the exercise of special electronic surveillance powers, the harm threshold should be set at a standard equivalent to '*seriously* undermining the utility' or 'causing *serious* and long-term impairment of' law enforcement agencies' ability to use the powers to combat serious crime.

8.77 An example of the type of disclosure that should be covered by this offence would be revealing that the Australian Federal Police was able to obtain and read messages from a specific type of 'encrypted' device used by major organised crime groups because the devices were actually controlled by a law enforcement agency.[523] It is not intended that conduct such as encouraging people to contact journalists using an encrypted platform be penalised in any way. Information that has already been disclosed officially or as part of a prosecution would not be penalised because of the defences that apply in those circumstances.

8.78 It is probably not as easy for a non-official to identify whether information would undermine the utility of the much broader category of methods connected to special powers granted to any agency to access information or to search people, places or things. Therefore, it will be rare for there to be a circumstance where there is sufficient evidence to show the person was aware of a substantial risk that the harm will occur and that, having regard to the circumstances known to them, it is unjustifiable to take the risk. Furthermore, where the exercise of these powers is overt and does not rely on covert technology or capabilities then a disclosure would not cause harm. Nevertheless, it is possible to envisage at least some circumstances where harm to a capability might occur, for example, in relation to ways to defeat special forensic capabilities used to analyse devices seized under a search warrant. If this category is to be included in the offence for non-officials, the harm threshold should be set at the same level as for electronic surveillance equivalent to 'seriously undermining the utility' or 'causing serious and long-term impairment of' law enforcement agencies ability to use the statutory power.

8.79 For officials, disclosures that impede the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth will be penalised under the new general offence if **Recommendation 11** is accepted. For non-officials, the harm threshold for such disclosures should be raised to the equivalent of 'seriously impeding' or 'seriously prejudicing' the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth.[524]

8.80 An example of when this offence would apply would be advising a person that they are about to be subject to a search warrant in order to given them the opportunity to hide or destroy evidence of offending.

8.81 I note that there is already a range of specific offences that apply to disclosures relating to the criminal justice system, including those for witness protection and perverting the course of justice as well as specific offences for disclosures connected to especially sensitive operations such as ASIO's special intelligence operations. These will continue to apply.

---

523 See, for example, Australian Federal Police (AFP), 'AFP-led Operation Ironside smashes organised crime in 2021' (Media Release, 21 December 2021).

524 Law Council of Australia, *Submission 19*, 37 [126]-[127].

Harm to the public

8.82 The fourth part of the current offence for non-officials is that:

> the communication of the information harms or prejudices the health or safety of the Australian public or a section of the Australian public.

8.83 This is part of the current offence for officials, and I have not recommended any changes to it with respect to officials. The Law Council suggested that this requirement be altered to require 'serious' harm to the health or safety of the Australian public or a section of the Australian public for disclosures by officials and non-officials.[525] 'Serious harm' to people means harm that endangers or is likely to endanger life or that is likely to be significant and longstanding.[526] That is a high threshold, particularly when, as discussed in **Chapter 5**, my understanding is that this element refers to matters that are widespread and threaten public safety or public health generally – rather than being akin to matters affecting an individual. On this basis, the offence already describes a serious harm to a critical national interest. However, if there is any doubt as to this reading then the offence should be redrafted to refer to 'serious harm' as suggested by the Law Council.

8.84 As mentioned in **Chapter 5**, it is difficult to identify many circumstances where the release of government information would actually harm or prejudice the health or safety of the Australian public or a section of the Australian public. This review did not specifically request examples of where this may occur and none were identified in the Revised Explanatory Memorandum for the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2018, but the ALRC *Secrecy Laws and Open Government in Australia* report provided one example:

> The ALRC has concluded that unauthorised disclosures of information that are likely to prejudice the protection of public health – for example, the location of national supplies of a vaccine being stockpiled in a secure location in case of national emergency – would also prejudice the protection of public safety.[527]

Penalty provisions for non-officials

8.85 Research on the effectiveness of criminal sanctions as a deterrent indicates that the issue is complex and that the relationship between penalty and deterrence is not linear.[528]

---

525 Law Council of Australia, *Submission 19*, 33-37 [102]-[128].

526 *Criminal Code* (n 513) Dictionary.

527 *ALRC 2009 Secrecy Laws Report* (n 477) 160 [5.76].

528 See, for example, Lawrence Sherman, 'Defiance, Deterrence, and Irrelevance: A Theory of the Criminal Sanction' (1993) 30(4) *Journal of Research in Crime and Delinquency* 445; Richard Johnstone and Rick

Nevertheless, penalties have a role in both deterrence and punishment and should reflect the level of criminal culpability as well as harm. Judges determine the actual penalty in individual cases taking the usual sentencing principles into account.[529] However, the maximum penalty set by the parliament should also have regard to deterrence, punishment and culpability in relation to the *class of people* subject to the offence, at least in cases like Part 5.6, where distinction between different classes of persons is an integral part of the statutory framework.

8.86 It is true that, in some cases, a disclosure by a non-official could result in the same harm to the national interest as the disclosure of the same information by an official. However, in the case of the government information that is the subject of the offences in Part 5.6, a non-official must first have received the information by virtue of a disclosure by a Commonwealth officer or person otherwise engaged to perform work for a Commonwealth entity. That official will almost certainly have access to a much larger volume of government information and has the ability to disclose it to any number of non-officials or, indeed, the world at large, thanks to modern technology. Access to a larger volume of government information and the ability to disclose to other non-officials (for example, if the first declines to publish) are both reasons the primary deterrent should be in relation to disclosures by officials.[530]

8.87 Furthermore, while both officials and non-officials bear a level of culpability for intentionally, knowingly or recklessly causing harm, there is an additional level of culpability for Commonwealth officers and others engaged to perform work for a Commonwealth entity because, by making the initial disclosure to a non-official, they have breached an important duty and trust that is part of being a Commonwealth officer or person otherwise engaged to perform work for the Commonwealth.

8.88 As noted earlier, the maximum penalty for disclosures by non-officials in Australia is currently higher than in comparable countries. The Law Council recommended reducing the penalty to 12-months imprisonment for all offences for non-officials. I consider that penalty too low as a maximum penalty for serious harm to security or defence or seriously undermining

---

Sarre, *Australian Institute of Criminology: Regulation: Enforcement and Compliance Report* (Report No 57, 2004) 7; Raymond Paternoster, 'How Much Do We Really Know about Deterrence?' (2010) 100(3) *Journal of Criminal Law & Criminology* 765; Daniel Nagin, 'Deterrence in the Twenty-First Century' (2013) 42(1) *University of Chicago Press* 199.

529 See, for example, *Elias v The Queen; Issa v The Queen* [2013] HCA 31. Also see *Crimes Act 1914* (Cth) ss 16A, 16B. See Chapter 6 for some discussion of sentencing principles and aggravating circumstances.

530 For example, in the case of *R v McBride (No 4)* [2024] ACTSC 147, Mr McBride disclosed classified information to two separate journalists who both declined to publish it (see [83]-[88]) before publishing some of it himself on a website (see [91]) and eventually providing the material to a third journalist who did publish some of it (see [99]-[102]).

electronic surveillance capabilities where the consequences of the commission of the offence are particularly damaging.[531]

8.89 In my view, the maximum penalties for non-officials should be approximately half the penalty for officials for a comparable offence in Part 5.6. For example, in accordance with **Recommendations 2** and **10**, the maximum penalty for an official who *intentionally* discloses information about the technologies, capabilities and methods used to exercise special electronic surveillance powers would be up to 10-years imprisonment. The maximum penalty for a non-official who *intentionally* seriously undermines the same capability should be 5 years. Recklessness for the same disclosure by an official would attract a maximum of 7 years and so for a non-official should be 3 years. Similarly, for the *reckless* disclosure by an official that impeded the prevention, detection (etc.) of a crime contrary to proposed general offence in s 122.4 (**Recommendation 11**), the maximum penalty would be 2 years, so for a non-official it should be one year.

8.90 If differential penalties for recklessness and knowledge/intent are adopted then provision should be made for alternative convictions.

Recommendation – offence for non-officials

8.91 Information disclosure offences for people who did not come by information in their capacity as an official or former official or person otherwise engaged to perform work for a Commonwealth entity should have an express harm element and should generally be narrower than offences for officials. This position is consistent with key former reviews, including those by the ALRC and a former INSLM. The current offence for non-officials is a mix of deemed harm (where the information has a security classification) and actual harm (3 other circumstances). This review recommends removing the deemed harm element and adjusting the other harm-based elements consistent with other recommendations in this report. Penalties should be adjusted to approximately half the maximum penalty for officials, recognising that the higher penalty for officials reflects a greater need for deterrence (as officials have access to more information and can disclose it to multiple non-officials) and a greater level of culpability among those who have voluntarily taken on a duty to serve the Commonwealth and then breached that duty and trust.

531 AGD, *A Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* (Guideline, September 2011) 38 [3.1.1].

RECOMMENDATION 12: The offence in s 122.4A for communications by non-officials should be modified so that:

- **classification markings do not form an element of the offence**
- **the current requirement that actual harm be established should be maintained and the offence apply to:**
  - **causing serious damage to the security or defence of Australia, with those terms defined as per Recommendation 6**
  - **seriously undermining the utility of the technologies, capabilities and methods used to exercise special statutory powers (per Recommendations 3 and 4)**
  - **seriously impeding the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth**
  - **prejudicing the health or safety of the Australian public or a section of the Australian public**
- **the maximum penalty should be approximately half the maximum penalty for a comparable communication by an official.**

Action should be taken to ensure that ABC and SBS staff and contractors are not inadvertently covered by the offences for officials as persons 'otherwise engaged to perform work for a Commonwealth entity'.

8.92 For the reasons given in **Chapter 6** I have recommended that 'dealing with' offences for non-officials should be removed (**Recommendation 8**). If that recommendation is not accepted then intention or knowledge would be the appropriate fault (mental) element for dealing-with offences by non-officials if they are to be retained. For the reasons given in **Chapter 4**, I have recommended that 'security classification' not be used as an element of an offence, including the offence for non-officials. If that recommendation is not accepted then intention or knowledge would be the appropriate fault (mental) element for this offence.

Chapter 9: Defences

9.1 There are 9 specific defences contained in Part 5.6 of the *Criminal Code*.[532] While all are within the scope of this review, the one that has drawn the most attention in this and previous reviews is s 122.5(6), which is concerned with actions occurring in the course of the business of reporting news where the 'journalist' involved reasonably believed that the action was in the public interest. This is often described as the 'journalist defence'. The government recently accepted a recommendation that this defence be used as a model for a public interest journalism defence in other secrecy laws.[533]

9.2 The 'journalist defence' is a defence. It currently requires the defendant to discharge an 'evidential burden' to enliven the defence before the prosecution has to disprove beyond reasonable doubt that the defence applies (most relevantly here, that the defendant did not reasonably believe their conduct was in the public interest). This is not the same as an *element* of the offence that requires the prosecution to prove in every case that a communication is not in the public interest – something that has been proposed to this review and to previous reviews.

9.3 Most of this chapter is about the 'journalist defence', including whether it should be augmented by a general public interest defence or a public interest *element* in the offences. Other defences, including a defence specific to lawyers, are dealt with at the end of the chapter.

The journalist defence

9.4 The special position of journalists and news media organisations and the need to ensure that investigative and prosecutorial policies take account of the public interest in maintaining a free press is recognised in the current ministerial direction given to the Australian Federal Police (AFP) about journalists and the current AFP sensitive investigations policy. As **Chapter 10** finds, these instruments and policies are useful, although, of course, they can be

532 The 'standard' defences in Part 2.3 of the *Criminal Code Act 1995* (Cth) ('*Criminal Code*') are also applicable.

533 Attorney-General's Department (AGD), *Review of Secrecy Provisions* (Final Report, 21 November 2023) 9, recommendation 8 ('*AGD Review of Secrecy Provisions*'). Also see Australian Government, *Response to the Parliamentary Joint Committee on Intelligence and Security Report: Inquiry into the Impact of the Exercise of Law Enforcement and Intelligence Powers on the Freedom of the Press* (Government Response, December 2020) 6–7, recommendation 7.

changed by the Executive. Regardless of the practical limits imposed by policy, the existence of a specific defence for journalists in the *Criminal Code* is a critical safeguard.

9.5 The 'journalist defence' applies to people 'engaged in the business of reporting news, presenting current affairs or expressing editorial or other content in news media', as well as administrative staff and certain others acting under the direction of a journalist, editor or lawyer. The defence applies only if the journalist reasonably believed that engaging in the conduct was in the public interest. 'Public interest' is not defined, but a small number of actions are expressly excluded from being regarded as in the public interest.[534]

9.6 Submissions to this review relating to the journalist defence and related public interest proposal can be broadly divided into the following categories:

- concerns about evidential burden resting with the accused
- a proposal that a public interest test be added as an *element* of offences or that a general public interest *defence* be added (that is, a defence not limited to journalists or staff)
- a proposal that the defence be reframed as an exception
- suggestions about how a 'journalist' should be defined.

9.7 Each of these is discussed below.

Evidential burden resting with the accused

9.8 For most defences, including the journalist defence, the evidential burden lies with the accused.[535] This raises 3 interrelated issues which were discussed in submissions: compatibility with Australia's international obligations under art 14(2) of the *International Covenant on Civil and Political Rights* (ICCPR); concerns that journalists may need to reveal their source in order to satisfy the defence; and concerns about how administrative and other support staff may be able to point to or adduce evidence about the state of mind of a

534 These exclusions relate to identifying an Australian Secret Intelligence Service (ASIS) or Australian Security Intelligence Organisation (ASIO) officer or agent or a person who is part of the witness protection program or if the conduct was engaged in for the purpose of assisting a foreign intelligence agency or military organisation. See s 122.5(7).

535 The defendant bears the evidential burden in relation to all of the defences for which s 122.5 provides, save for where a defence under s 122.5(1), (3)(a)(i)–(iii), (3)(b), (4) or (4A) is raised by a person mentioned in s 122.5(3)(a)(i)–(iii) (certain integrity agency officials) of the *Criminal Code* (n 532). Also see *Criminal Code* (n 532) s 13.3.

journalist they were assisting. Before discussing these issues, it is helpful to first briefly describe what an 'evidential burden' is.

What is an evidential burden?

9.9 Broadly, an 'evidential burden' means that a defendant needs to provide some evidence to suggest that there is a 'reasonable possibility' that the relevant matter exists (or, where relevant, does not exist).[536] The evidential burden is described in *Cross on Evidence* as follows:

> Where the accused bears an evidential burden, but not a legal burden, the accused may discharge it by satisfying the following test: 'is there evidence which, taken at its highest in favour of the accused, would lead a jury, properly instructed, to have a reasonable doubt that each of the elements of the defence has been negatived?[537]

9.10 For example, a journalist seeking to rely on the 'journalist defence' would need to be able to point to evidence to suggest that there was a reasonable possibility that they 'reasonably believed that engaging in that conduct was in the public interest'. Producing evidence that there is a 'reasonable possibility' is a lower standard than requiring the defendant to positively prove a matter. If the defendant can point to sufficient evidence to show there is a 'reasonable possibility' of the relevant matter then the onus shifts to the prosecution to disprove the matter to the legal standard of beyond reasonable doubt.

9.11 This means that it is necessary to point to some evidence of a belief (held by the individual) as well as evidence that the belief was reasonable. Whether the belief is reasonable will require pointing to one or more public interest. In most cases, if evidence of a public interest is accepted, it will be relatively easy to infer that this was a reason that the journalist engaged in the conduct.

9.12 The Law Council of Australia suggested that the types of matters that a court might consider in determining whether an unauthorised disclosure is in the public interest include:

- promoting open discussion of public affairs, enhancing government accountability or contributing to positive and informed debate on issues of public importance
- informing the public about the policies and practices of agencies in dealing with members of the public
- ensuring effective oversight of the expenditure of public funds
- the information is personal information of the person to whom it is to be disclosed

536 See *Criminal Code* (n 532) s 13.3.

537 JD Heydon, *Cross on Evidence* (Lexis Nexis Australia, 14th ed, 2024) [7050] citing *Braysich v R* (2011) 243 CLR 434, [36] (French CJ; Crennan and Kiefel JJ).

- revealing or substantiating that an agency (or a member of an agency) has engaged in misconduct or negligent, improper or unlawful conduct.[538]

9.13 Although the matter has not been tested in relation to the meaning of 'public interest' in the journalist defence in s 122.5(6), it seems likely that these would be the sorts of factors which would be relevant, although, of course, any defence is dependent on the specific facts of the case.

9.14 Requiring a person to discharge an evidential burden is not quite the same as a 'reversal of the onus of proof'. The legal burden for a criminal offence is 'beyond reasonable doubt': this is what the prosecution is required to establish for every element of the offence and for any defence or exception for which the defendant has discharged the evidential burden. The defendant does not need to prove beyond reasonable doubt that they had a reasonable belief that engaging in that conduct was in the public interest; they only need to point to evidence that, taken at its most favourable, suggests there is a 'reasonable possibility' that this was the case.[539]

International obligations and the evidential burden

9.15 Because the evidential burden rests with the defendant, art 14(2) of the ICCPR needs to be considered. It provides that:

> everyone charged with a criminal offence shall have the right to be presumed innocent until proved guilty according to law.

9.16 In other words, art 14(2) of the ICCPR describes the right to the presumption of innocence. This includes the imposition of a burden on the prosecution to prove the charge and that the presumption of innocence exists until the charge has been proven beyond reasonable doubt.[540]

9.17 Laws that shift some of the burden of proof to the defendant are not necessarily incompatible with art 14(2) as long as the law pursues a legitimate objective, is rationally connected to that objective and is a proportionate means of achieving that objective.[541] Imposing an evidential burden on the defendant to adduce or point to evidence making out a defence (following

538 Law Council of Australia, *Submission 19*, 44 [160].

539 AGD, *Submission 7*, 20-1[95]–[96].

540 There are other aspects to this right including independence of the judge and a duty on public authorities to refrain from prejudicing the outcome of the trial. See Manfred Nowark, *UN Covenant on Civil and Political Rights: CCPR Commentary* (Engel, 2nd rev ed, 2005) 329–31.

541 Parliamentary Joint Committee on Human Rights (PJCHR), Parliament of Australia, *Human Rights Scrutiny Report* (Report No 3, 27 March 2018) 239 [2.344] ('*PJCHR Human Rights Scrutiny Report 3*').

which the burden shifts to the prosecution to disprove the matter) is more likely to be compatible with the presumption of innocence than a requirement that the defendant prove an element of the defence beyond reasonable doubt.[542]

9.18 The Attorney-General's Department (AGD) considers that there is no inconsistency between the way the defences in Part 5.6 of the *Criminal Code* currently operate and art 14 of the ICCPR:

> The department considers that applying an evidential burden to the relevant defences in section 122.5 is compatible with Article 14 of the ICCPR. It is to pursue a legitimate aim and that the manner in which that aim is pursued is reasonable, necessary and proportionate.[543]

9.19 In contrast, the Australian Human Rights Commission (AHRC) was of the view that shifting the burden of proof risks 'interfering with the right to be presumed innocent'.[544]

9.20 AGD highlighted that placing an evidential burden on a defendant is not the same as *reversing* the legal burden of proof:

> Imposing an evidential burden on a defendant who wishes to rely on any exception or exemption to an offence does not reverse the legal burden of proof for the offence. An evidential burden is 'the burden of adducing or pointing to evidence that suggests a reasonable possibility that the matter exists or does not exist' (subsection 13.3(6) of the Criminal Code). As set out in section 13.1 of the Criminal Code, the prosecution bears a legal burden of proving every element of an offence relevant to the guilt of the person charged and also bears a legal burden of disproving any matter in relation to which the defendant has discharged an evidential burden.[545]

9.21 AGD noted decisions by the European Court of Human Rights dealing with a similar provision. That court has found the 'shift of the burden to the defence is compatible with a presumption of innocence after a prima facie case has already been made against the accused'.[546]

---

542 *R v DPP, Ex parte Kebilene* [2000] 2 AC 326, 379; *R v Lambert* [2001] UKHL 37, [37]–[41].

543 AGD, *Submission 7*, 20-1 [95].

544 Australian Human Rights Commission (AHRC), *Submission 17*, 24 [96]. The commission also considers that shifting the burden of proof imposes an 'unreasonable burden on the freedom of expression'. See Chapter 3 for discussion of the right of freedom of expression.

545 AGD, *Submission 7*, 21 [96].

546 AGD, *Submission 7*, 21 [97] citing *Telfner v Austria* (2001) EHRR 7, [18]; *Poletan and Azirovik v 'the former Yugoslav Republic of Macedonia'* [2016] ECHR 417, [63]–[67].

9.22 In giving reasons why it was appropriate to place an evidential burden on the defendant for the journalist defence, AGD pointed to the department's *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*, which indicates that:

> a matter should only be included in an offence-specific defence, as opposed to being specified as an element of the offence, where:
>
> - it is peculiarly within the knowledge of the defendant, and
> - it would be significantly more difficult and costly for the prosecution to disprove than for the defendant to establish the matter.
>
> Where it is intended to place the burden of proof on the defendant by creating an offence-specific defence, this should be clear on the face of the legislation. The explanatory material should also explain the reasons for placing the burden of proof on the defendant.[547]

9.23 Several submissions took a different view as to this justification. For example:

- AHRC noted that 'claims of greater convenience or ease for the prosecution in proving a case will be insufficient, in and of themselves, to justify a limitation on the defendant's right to be presumed innocent'.[548]
- The Alliance for Journalists' Freedom (AJF) added that it did not consider the argument that a defendant may be better placed to prove a particular matter to be a sufficient (or effective) reason for placing the burden on the defendant as 'question of convenience to the prosecutor'.[549]
- Australia's Right to Know (ARTK) submitted that this evidential burden means the defendant 'comes before the jury not as a person to be presumed innocent but a person presumed to have a case to answer'.[550] In the context where the journalist is the defendant, ARTK suggested that this erosion of rights could also extend to their implicated colleagues, such as editors, in-house lawyers and administrative staff.[551]

9.24 During the passage of the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 (EFI Bill), the Parliamentary Joint Committee on Human Rights (PJCHR), the Parliamentary Joint Committee on Intelligence and Security (PJCIS) and the Senate Standing Committee for the Scrutiny of Bills (Scrutiny of Bills Committee) considered

---

547 AGD, *A Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* (Guideline, September 2011) 50 ('*Guide to Framing Commonwealth Offences*').

548 AHRC, *Submission 17*, 8–9.

549 Alliance for Journalists' Freedom (AJF), *Submission 11*, [8.5].

550 Australia's Right to Know (ARTK), *Submission 12*, 7.

551 ARTK, *Submission 12*, 10–11.

compatibility with art 14(2). The committees observed that the evidential burden of proof was a critical issue to submitters,[552] and provisions requiring defendants to carry an evidential burden of proof limits the right to be presumed innocent until proven guilty as provided for in art 14(2) of the ICCPR.[553]

9.25 In its subsequent report, the PJCHR further observed that:

> The justification for reversing the evidential burden of proof is generally that the defendant 'should be readily able to point to' the relevant evidence or the defendant is 'best placed' to know of the relevant evidence. However, this does not appear to be sufficient to constitute a proportionate limitation on human rights. It was unclear that reversing the evidential burden is necessary as opposed to including additional elements within the offence provisions themselves.[554]

9.26 The PJCIS did not make any specific recommendations on this issue (except in relation to integrity officials). The Scrutiny of Bills Committee remained of the view that it was not appropriate to 'reverse the evidential burden of proof' in relation to the offence-specific defences.[555]

Finding on evidential burden and article 14

9.27 Placing any part of the burden on the defendant engages art 14(2) of the ICCPR. It then becomes necessary to consider whether the imposition pursues a legitimate objective, is rationally connected to that objective and is a proportionate means of achieving that objective.

9.28 The objective being pursued appears to be ensuring that criminal trials run efficiently. This is a legitimate objective. Imposing an evidential burden on the defendant where a matter is 'peculiarly within the knowledge of the defendant' and where it would be 'significantly more difficult and costly for the prosecution to disprove than for the defendant to establish the matter' is rationally connected to that objective.[556] The real question is whether this outcome is *proportionate*. To answer this, I must take into account the overall way that the law on defences operates for Commonwealth offences in Australia.

---

552 Parliamentary Joint Committee on Intelligence and Security (PJCIS), Parliament of Australia, *Advisory Report on the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (Report, June 2018) 84–90 ('*PJCIS EFI Bill Report*); PJCHR, *Human Rights Scrutiny Report* (Report No 2, 13 February 2018) 15-16 ('*PJCHR Human Rights Scrutiny Report 2*'); Senate Standing Committee for the Scrutiny of Bills (Scrutiny of Bills Committee), Parliament of Australia, *Scrutiny Digest 4 of 2018* (28 March 2018) 21 ('*Scrutiny of Bills Digest*').

553 *PJCHR Human Rights Scrutiny Report 2* (n 552) 13 [1.46].

554 *PJCHR Human Rights Scrutiny Report 3* (n 541) 15 [1.53].

555 *Scrutiny of Bills Digest* (n 552) 26-8 [2.47]–[2.51].

556 *Guide to Framing Commonwealth Offences* (n 547) 50.

9.29 By way of general context, in criminal trials in Australia the prosecution is required to put its case first and to prove beyond reasonable doubt every element of the offence. The prosecution is also under a duty to produce any exculpatory material and, with some exceptions, to call all witnesses who can give relevant testimony. The defence can cross-examine prosecution witnesses and adduce its own evidence. Then, as discussed above, the defendant can seek to rely on a defence by pointing to or adducing evidence that, taken at its most favourable, suggests there is a 'reasonable possibility' that the defence is available. The burden then rests on the prosecution to prove beyond reasonable doubt that every element of the defence is negated. In most circumstances this is a proportionate restriction on the right in art 14(2). However, in the case of journalists, additional consideration is needed to assess whether there is a specific reason they may be unable to bring relevant material in their defence.

Concern that a journalist may need to reveal their source

9.30 Being able to provide a meaningful and credible assurance of confidentiality to a source is essential for public interest journalism.[557] Protecting sources is a key tenet of the Media, Entertainment and Arts Alliance (MEAA) Journalists Code of Ethics.[558] Media organisations made strong submissions about their concern that, in at least some situations, the current journalist defence may place a journalist in the position of having to choose between revealing a source and not raising a defence otherwise available to them.[559] This concern was described in some detail in the ARTK submissions. My understanding of the argument that ARTK put forward is as follows. The test of 'reasonable belief' has both an objective element (reasonable) and a subjective element (actual belief). To discharge the evidential burden in relation to their state of mind (actual belief that their conduct was in the public interest) it may be necessary for a journalist to give evidence about their state of mind. Furthermore, to establish that their belief was objectively reasonable, they may need to rely on an argument that the (objective) reasonableness of their belief was connected to the credibility of the source of the information. Defendants are not obliged to give evidence, but if they do they can be cross-examined. This therefore raises a risk that a journalist might be cross-examined as to their source, which is likely to be relevant to both the subjective and the objective

557 ARTK, *Submission 12*, 8 [29].

558 Media, Entertainment and Arts Alliance (MEAA), *Submission 9*, 4.

559 Mr Peter Greste, AJF, *Public hearing transcript*, 26 March 2024, 115–21; Ms Lilia Anderson, MEAA, *Public hearing transcript*, 26 March 2024, 118; Mr Robert Todd, ARTK, *Public hearing transcript*, 26 March 2024, 122.

reasonableness of their belief – journalists should not be expected to reveal a source, even in their own defence, as doing so is contrary to their professional and ethical obligations.[560]

9.31 Every Australian jurisdiction has journalist shield laws that provide some protection against the disclosure of sources. ARTK notes that these laws are not nationally consistent and generally provide the judge with discretion to order the disclosure of a source if the public interest in disclosure outweighs countervailing factors. ARTK accepted that this risk would not arise in every case but submitted that the mere fact that it cannot be ruled out results in a chilling effect.[561] ARTK's preferred solution is to reframe the offences so that the prosecution is required to prove beyond reasonable doubt that a disclosure was *not* in the public interest in every prosecution and also to maintain a specific defence for journalists who reasonably believed they were acting in the public interest. I note that even if the law was reframed in that way, it would not remove the possibility that a judge applying the shield laws in the relevant jurisdiction would order the disclosure of information about a source.

Finding on journalist sources

9.32 I accept that any possibility that a journalist might be questioned in the witness box about their source is a real concern to journalists and media organisations. I accept the concern a situation like that described by ARTK might arise could weigh heavily on a journalist and may have a 'chilling effect'. However, there are a number of steps and safeguards in the criminal justice process that need to be considered. In combination, they make the chance of a journalist being compelled to disclose a source in order to discharge an evidential burden for this defence remote, although I also accept that the risk (albeit remote) of this may also have the effect of constraining the way that a journalist might seek to defend any prosecution.

9.33 First, assuming that the Commonwealth Director of Public Prosecutions (CDPP) is satisfied that a prosecution is in the public interest and that the Attorney-General has exercised his or her discretion to consent to a prosecution (see **Chapter 10**), the prosecution must put its case 'fully and fairly' before the defendant opens his or her case. As ARTK noted in its original submission, it is only in exceptional circumstances that a judge will allow a prosecution to reopen its case, and it is unlikely to be an 'exceptional circumstance' to fail to foresee a likely defence – such as a journalist raising the journalist defence.[562] As a practical matter, this means that the prosecution will usually seek to disprove that a journalist acted with a reasonable belief that their conduct was in the public interest in its case. As ARTK pointed

560 ARTK, *Supplementary submission 21*, 5–6. See also ARTK, *Submission 12*, 7-15 [25]–[70].

561 ARTK, *Submission 12*, 7-15 [25]–[70]; ARTK, *Supplementary submission 21*, 6 [48]. See also Ms Lilia Anderson, MEAA, *Public hearing transcript*, 26 March 2024, 118.

562 ARTK, *Submission 12*, 11-12 [49]–[53].

out, it may be difficult for the prosecution to show there was not a 'reasonable belief' to the legal standard.[563]

9.34 Second, the defence can cross-examine prosecution witnesses if it thinks doing so will assist its case or is necessary to ensure the evidential burden is discharged without their client being called. For example, witnesses giving evidence for the prosecution could be asked about whether the publication of the relevant information was referred to in public debate or in notes or statements prepared by an agency for ministers or senior officials to enable them to respond to questions about alleged improper or unlawful conduct (this goes to the objective reasonableness). It may then be enough to adduce or point to evidence from other sources that a reasonable journalist in the position of the defendant would consider publishing such stories as being in the public interest and that from this it can be inferred (to the evidential burden standard) that there is a 'reasonable possibility' the defendant had the requisite state of mind (subjective belief). Indeed, it might be argued that the defendant's subjective belief could be sufficiently inferred from objective matters such as the subject matter of the stories.

9.35 As noted above, a court is likely to take a fairly wide view of factors that may be in the public interest. It seems likely that most defences involving 'public interest journalism' could point to at least 'slender evidence' that 'taken at its most favourable to the accused' suggests a 'reasonable possibility' the journalist reasonably believed their conduct was for the purpose or purposes that included one or more of these reasons. In discharging an evidential burden, it is not incumbent on the defendant to point to evidence that their conduct was *actually* in the public interest; only that they had some reasonable basis for that belief. Factors unknown to the defendant, such as a 'mosaic effect' or the capabilities and intentions of an unknown foreign intelligence agency, would not be relevant (see **Chapter 2** on the mosaic effect).

9.36 Third, in the event a journalist does decide to give evidence in their own defence, the shield laws provide a further layer of protection, albeit not a complete guarantee. Reviewing the various shield laws is beyond the scope of this review. It is enough to note that there are such laws and that their effect is to provide a level of protection to journalists' sources. That the laws ultimately retain an element of judicial discretion to determine whether the public interest in disclosure outweighs countervailing factors is not inappropriate and not outweighed by the remote risk presented by the way the journalist defence in s 122.5(6) is framed.

9.37 It follows from this discussion that the concerns specific to journalists' sources are not sufficient to alter the general conclusion on art 14(2) of the ICCPR discussed above: it is not inconsistent with that right to impose an *evidential burden* on journalists when the full context of the Australian criminal justice system is considered.

563 ARTK, *Submission 12*, 13 [60].

Administrative staff and the current journalist defence

9.38 The 'journalist defence' in s 122.5(6)(a) (which requires that the person had a reasonable belief that engaging in the relevant conduct was in the public interest) does not only apply to journalists. It applies to any person who communicated or dealt with the information in their work in the business of reporting news and so on. This includes administrative staff. However, perhaps in recognition that it is not always reasonable to expect an administrative staff member to weigh the public interest when doing routine tasks under direction (such a copying or storing documents), there is also a special defence for administrative staff. That defence, in s 122.5(6)(b), applies when:

> (b) the person:
>
> (i) was, at that time, a member of the administrative staff of an entity that was engaged in the business of reporting news, presenting current affairs or expressing editorial or other content in news media; and
>
> (ii) acted under the direction of a journalist, editor or lawyer who was also a member of the staff of the entity, and who reasonably believed that engaging in that conduct was in the public interest (see subsection (7)).

9.39 In other words, to benefit from the defence, the administrative staff member needs to be able to adduce or point to evidence that they were a member of the administrative staff of a news media organisation (etc.) and that:

- they were acting under the direction of a journalist, editor or lawyer who was also a staff member of the entity; and
- the other person (the journalist editor or lawyer) reasonably believed that having the administrative staff member engage in the conduct was in the public interest.[564]

9.40 It is the last part of this test that ARTK contends is problematic. The defence relies on a belief that is 'subjectively held not by the defendant but by someone else entirely'.[565] In essence, the concern is with how Person A (administrative staff) can show that Person B (journalist, lawyer or editor) believed that Person A engaging in the conduct was in the public interest. This, ARTK notes, may be particularly difficult if Person B is unwilling or unable to give evidence about why they (subjectively) believed the actions of Person A were in the public interest.[566]

---

564 *Criminal Code* (n 532) s 122.5(6)(b).

565 ARTK, *Submission 12*, 10 [41].

566 ARTK, *Submission 12*, 10-11[41]–[47]. Note that the additional defence for administrative staff was inserted on the basis of a submission to the PJCIS by the Joint Media Organisations during the consideration of the National Security Legislation Amendment (Espionage and Foreign Interference)

9.41 It will not always be necessary for Person B to be willing or able to give evidence. As discussed above, the discharge of an evidential burden is not a high bar. Person A only needs to be able to point to evidence that suggests a reasonable possibility that the lawyer, journalist or editor had the reasonable belief. Because of s 122.5(6)(a), an administrative staff member could also rely on the defence that they themselves reasonably believed that their conduct was in the public interest.

9.42 Nevertheless, given the way the defence specific to administrative staff in s 122.5(6)(b) is drafted, it effectively requires the administrative staff member to consider whether the journalist, editor or lawyer who is giving them the direction believes it to be in the public interest. This appears an odd result.

9.43 The Supplementary Explanatory Memorandum to the EFI Bill is unclear as to whether the policy intention was that the administrative staff members be protected only if the journalist, editor or lawyer held a reasonable belief as to the public interest or whether administrative staff should be protected whenever acting under a direction:

> The defence will contain an additional limb applying to administrative staff of an entity that was engaged in reporting news, presenting current affairs or expressing editorial or other content in news media who acted under the direction of a journalist, editor or lawyer who reasonably believed that dealing with or holding the information was in the public interest. This will ensure that any member of the administrative staff is protected if he or she acted under the direction of another person. This is consistent with the amendments requested by the Joint Media Organisations in Submission 9.2 to the PJCIS inquiry.[567]

9.44 Regardless of what the Revised Explanatory Memorandum provides, the words of the Act are clear – the defence is only available if the journalist, editor or lawyer who gave the direction reasonably believed that the administrative staff member was engaging in the conduct in the public interest. However, before concluding that change is needed, it is necessary to consider the offence to which the defence is directed and the sort of scenario where the defence may be called upon.

9.45 As discussed in **Chapter 8**, the offence for non-officials in s 122.4A is currently a mix of a deemed harm offence (the circumstance that the information is 'classified information' per s 122.4A(d)(i)) and a harm-based offence (the results in s 122.4A(d)(ii)–(iv)).

Bill 2018 ('*EFI Bill*'). That submission proposed that the defence apply to a person who reasonably believed that dealing with the information was in the public interest *or was acting* at the direction or under instruction of a person who held such a belief. See Joint Media Organisations, Submission No 9.2 to PJCIS, *Inquiry into the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (13 March 2018) 5.

567 Supplementary Explanatory Memorandum, *EFI Bill* (n 566) 97 [635]. See also Revised Explanatory Memorandum, *EFI Bill* (n 566) 331 [1672].

9.46 For the deemed harm component (that the information is classified), it is possible to see how an administrative staff member might be reckless as to whether a document that they were asked to deal with or communicate has a classification marking on it. For example, a journalist or editor might give the staff member a document marked 'secret' and ask them to provide a copy of it to a lawyer working in the same entity so that advice can be provided about the offences in Part 5.6. As discussed in **Chapter 4**, to establish recklessness the prosecution would need to prove beyond reasonable doubt that the administrative staff member was aware of a substantial risk that the information was classified information and that, having regard to the circumstances known to him or her, it was unjustifiable to take the risk. Establishing that the administrative staff member had seen the classification marking or had heard others describing the information as classified information may be sufficient to satisfy this.[568] It would not be necessary to show that the administrative staff member had read the document or considered whether harm might arise from that copying or communicating. In this deemed harm scenario, it does not seem reasonable for the administrative staff member to have to question the journalist or editor about whether they believe copying or communicating the document to the lawyer is in the public interest.

9.47 In light of current AFP investigative polices and the Prosecution Policy of the Commonwealth, the chance of an administrative staff member being prosecuted in such a scenario seems low. Nevertheless, as a matter of principle, it is difficult to see how it is necessary or proportionate to effectively impose a duty under the criminal law to consider the motivation of others on a non-government staff member who is dealing with information to perform a routine administrative task in the course of their employment, without any test of whether their actions may result in actual harm.

9.48 This can be contrasted with a situation where an administrative staff member was charged with a communication offence under s 122.4A(1) as modified by **Recommendation 12** of this review. If that recommendation is implemented, an administrative staff member would only commit an offence if they communicated information and were at least aware of a substantial risk that their conduct would have one or more of the following results and that, having regard to the circumstances known to him or her, it was unjustifiable to take the risk:

- seriously damaging the *security* or *defence* of Australia
- seriously undermining the utility of the technologies, capabilities and methods used to exercise special statutory powers
- seriously impeding the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth

568 Strict liability applies in relation to the mental element, but the prosecution would also have to prove the physical element i.e. that the information actually was properly classified information – see Chapter 4.

- prejudicing the health or safety of the Australian public or a section of the Australian public.

9.49 These are serious results, and a person who is *actually* aware of a substantial risk that their conduct may result in such serious harm can reasonably be expected to take some action. What that action is will depend on the circumstances known to him or her.

9.50 The effect of **Recommendation 8** will be to remove the 'dealing with' offence for non-officials. For administrative staff this means that most routine administrative actions, such as storing or copying a document in the course of their work, will no longer be criminalised.

Finding in relation to defence for administrative staff

9.51 If **Recommendations 1, 8** and **11** are accepted and the deemed harm element (classified information) and the 'dealing with' offence are removed from s 122.4A then, although the operation of the defence will be awkward, it provides sufficient protection for administrative staff in combination with the much narrower offence provisions.

9.52 If **Recommendations 1**, **8** or **11** are not accepted then the offence in s 122.4A and the defence for administrative staff should, at a minimum, be revised so that, in combination, administrative staff are only liable for actions that cause actual harm and that there remains a defence for where they or the person whose direction they were acting under reasonably believed the conduct to be in the public interest. A neater alternative would be to simply make the defence for administrative staff that they were acting in the course of their duties, similar to the defence for Commonwealth officials.

Proposal that a public interest test be added

9.53 Several submitters suggested that instead of, or in addition to, a defence for journalists and administrative staff that relies on an individual having a reasonable belief that their action was in the public interest, there should be a public interest test in the offence itself[569] – in other words, an *element* of the offence that requires the prosecution to prove beyond reasonable doubt that a particular disclosure (or dealing) was not in the public interest. If this test was introduced, the prosecution would have to prove a negative beyond reasonable doubt, without the accused first discharging an evidential burden. Alternatively (or in addition), it has been suggested that there should be a general public interest *defence* that applies to anyone (including officials) if their disclosure was 'in the public interest'.

---

569 Human Rights Law Centre (HRLC), *Submission 14*, 14–15. ARTK, *Submission 12*, 5; Law Council of Australia, *Submission 19*, 41–2.

9.54 This review is not the first time these types of proposals have been considered. In some previous reviews it has been described as a general public interest defence and in others as a new element of the offence:

- In its inquiry into the EFI Bill, the PJCIS received multiple submissions about media and public interest defences.[570] The Committee concluded that the other defences in the EFI Bill provided sufficient protections and did not recommend the inclusion of a more broadly drafted public interest defence.[571]
- The *Comprehensive Review of the Legal Framework of the National Intelligence Community* (Comprehensive Review Report) received submissions, including from Dr Hardy and Professor Williams, the Human Rights Law Centre (HRLC) and others, on creating broader public interest disclosure exceptions. The Comprehensive Review Report also contains a summary of earlier consideration of this issue from other reviews that occurred before Part 5.6 of the *Criminal Code* was enacted, including by the Gibbs Committee; the Australian Law Reform Commission; the Samuels and Codd Commission of Inquiry; the PJCIS; and the Senate Select Committee on Public Interest Whistleblowing. The Comprehensive Review Report rejected a broader 'public interest defence' largely on the basis that an effective public interest disclosure scheme was a better mechanism in the context of national intelligence community information.[572]
- In 2020 the PJCIS *Inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press* (PJCIS Inquiry into Press Freedoms) described the 'journalist defence' in s 122.5(6) as a model that could be used in creating defences for other secrecy provisions.[573] The Committee did not recommend any expansion of the defence or converting the defence to an element, despite several submissions proposing expansion and some recommending it be converted into an element.[574]

---

570 See, eg, *PJCIS EFI Bill Report* (n 552) 166-8 [5.34]–[5.39], 172, 185, recommendation 27.

571 *PJCIS EFI Bill Report* (n 552) 187 [5.101].

572 Dennis Richardson, *Comprehensive Review of the Legal Framework of the National Intelligence Community* (Final Report, December 2019) 127-8 [35.174]–[35.179], recommendation 144 ('*2019 Comprehensive Review*').

573 The PJCIS recommended the government give consideration to whether defences for public interest journalism should be applied to other secrecy offences within relevant Commonwealth legislation. The Committee said any additional defences should be based on the defence provided by s 122.5(6) of the *Criminal Code* (n 532): see *PJCIS EFI Bill Report* (n 552) 83 [3.198], recommendation 7.

574 AHRC, Submission No 8 to PJCIS, *Inquiry into the impact of the exercise of law enforcement and intelligence powers on the freedom of the press* (25 July 2019) 7 ('*PJCIS Inquiry into Press Freedoms*'); Australian Lawyers Alliance, Submission No 5 to *PJCIS Inquiry into Press Freedoms* (24 July 2019) 6 [7]; Law Council of Australia, Submission No 40 to *PJCIS Inquiry into Press Freedoms* (7 August 2019) 26–9.

- In its 2021 report into *Freedom of the Press*, the (then) Senate Environment and Communications References Committee suggested that there is 'scope to expand the legislative protections' provided by s 122.5.[575] The Committee drew on submissions by Dr Hardy and Professor Williams, who proposed a broader approach to public interest protections so that unauthorised disclosure offences would include a limited public interest exemption 'permitting the publication of information in the "public interest"'.[576]
- The AGD Review of Secrecy Provisions supported the current specific defence for public interest journalism but did not recommend a wider public interest defence or listing public interest factors.[577]

9.55 Similar arguments to those put to previous reviews were also raised in this review.

9.56 HRLC recommended a general public interest defence to act as a 'defence of last resort', particularly where the technical requirements of the other defences may not have been met. HRLC advocates for the defence to apply to current and former officials as well as non-officials.[578]

9.57 ARTK suggested recasting the offence so that it contains a pubic interest element:

> [it] accords with the basic liberal democratic principle that it is for the State to clearly establish why the public *should not* be told matters relating to the affairs of its own government and that otherwise there is a presumption that the public *should and must be told* [emphasis in original].[579]

9.58 The effect of this proposal, according to ARTK, is that what is or is not in the public interest would be a question of objective fact that does not rely on the subjective motivations or beliefs of a journalist or any other defendant. On this approach they say the lack of public interest would need to be clearly articulated rather than be said to be implicit where the disclosure was contrary to an existing offence provision.[580]

9.59 The Law Council recommended a general public interest disclosure defence to the secrecy provisions where, on balance, the disclosure would be in the public interest in relation to the

---

575 Senate Environment and Communications References Committee, Parliament of Australia, *Freedom of the Press* (Report, May 2021) 43 [3.59].

576 Dr Keiran Hardy and Professor George Williams AO, Submission No 2 to Senate Environment and Communications References Committee, Parliament of Australia, *Freedom of the Press* (1 August 2019) 11.

577 *AGD Review of Secrecy Provisions* (n 533) 44–5.

578 HRLC, *Submission 14*, 14–15.

579 ARTK, *Submission 12*, 16 [79].

580 ARTK, *Submission 12*, 16–17.

activities of a wider range of civil society actors (including academics and public commentators who may not fall within the definition of persons engaged in the business of reporting news).[581]

9.60 AJF and MEAA focused largely on journalists, recommending that the evidential burden for the current defence not rest on the defendant[582] and that the *Criminal Code* should provide exemptions for journalists who are acting in the public interest and who disclose information that causes no actual harm to national security.[583]

Hate Symbols Act model

9.61 Since the previous reviews of secrecy offences which considered a general public interest defence, the Commonwealth Parliament recently passed the *Counter-Terrorism Legislation Amendment (Prohibited Hate Symbols and Other Measures) Act 2023* (Cth) (*Hate Symbols Act*).

9.62 The drafting of the *Hate Symbols Act* is quite complex. ARTK described it as 'convoluted'.[584] AJF agreed that it was not clearly written and that:

> you do effectively have to be a lawyer to navigate it in a reasonable way. And even then, it's not quite clear at first blush what it's saying.[585]

In contrast, Dr Dalla-Pozza thought the formulation of the exception in the *Hate Symbols Act* operates to 'make the law clearer on the page', as it lets the 'ordinary lay person … have a better sense of what harm the Parliament is trying to prevent'.[586]

9.63 The *Hate Symbols Act* introduced new offences into the *Criminal Code* prohibiting the public display or trading in certain Nazi and terrorist organisation symbols. These provisions contain both exceptions and defences. For example, the public display of a Nazi symbol is prohibited but there is an exception if a reasonable person would consider that the display is for religious, academic, educational, artistic, literary or scientific purpose and not contrary to the public interest. There is also an exception for display of a prohibited symbol for the purpose of news or current affairs reporting by a 'person working in a professional journalistic

581 Law Council of Australia, *Submission 19*, 42.
582 MEAA, *Submission 9*, 6; AJF, *Submission 11*, [8.1]–[8.10].
583 AJF, *Submission 11*, [8.9].
584 ARTK, *Supplementary submission 21*, [60]. Additional concerns raised by ARTK about the suitability of the model are at ARTK, *Supplementary submission 21*, 7–8.
585 Mr Robert Todd, ARTK, *Public hearing transcript,* 26 March 2024, 131.
586 Dr Dominique Dalla-Pozza, Australian National University, *Public hearing transcript,* 25 March 2024, 53.

capacity' 'in the public interest'. There is also a defence available if the person genuinely engages in the conduct for the purpose of opposing Nazi ideology, fascism or a related ideology.[587]

9.64 The Law Council contends that the drafting of the *Hate Symbols Act* means that the new offences for the display or trading in prohibited symbols 'require the prosecution to prove that a reasonable person would consider that the public display [of the symbol] was not done for an education or academic purpose in the public interest'.[588] This is correct, but the defendant would first have to discharge the evidential burden.[589] AJF suggested the *Hate Symbols Act* might be a reasonable model for an exception for journalists acting in the public interest.[590]

9.65 The *Hate Symbols Act* is a different model for addressing public interest than the secrecy offences in Part 5.6. It is a model that I considered as a possible new model for the secrecy offences in the course of this review, particularly as it is parliament's most recent example of public interest exceptions and defences.

9.66 However, it is important to recognise some important differences in the different crimes, including the different circumstances in which the offences arise. This was noted by AFP. At the public hearing AFP said that it is difficult to compare the *Hate Symbols Act* with the secrecy offence legislation because 'the objective of those two pieces of legislation are very different, in our view, in terms of the proposition of a carve out versus defence'.[591]

9.67 The *Hate Symbols Act* offences are offences directed at specific symbols used for certain purposes. For example, the display of Nazi symbols offence only occurs when a reasonable person would consider the display:

- involves the dissemination of ideas based on racial superiority or racial hatred, or
- could incite another person to offend insult, humiliate or intimidate a person because of their race, or

587 *Criminal Code* (n 532) ss 80.2H(1), (9), (10)(f).
588 Law Council of Australia, *Submission 19*, 41 [146].
589 This is because s 13.3 of the *Criminal Code* places the evidential burden on the accused in relation to exceptions as well as defences.
590 Ms Phyllida Behm, AJF, *Public hearing transcript*, 26 March 2024, 131.
591 Mr Stephen Nutt, Acting Assistant Commissioner, Australian Federal Police (AFP), *Public hearing transcript*, 25 March 2024, 97.

- could advocate hatred based on race, religion or nationality; or incites offending, insulting or humiliating or using force against a targeted group.[592]

9.68 Even when those circumstances apply, the public display of otherwise prohibited symbols is not an offence if a reasonable person would consider that the display is for religious, academic, educational, artistic, literary or scientific purpose and not contrary to the public interest. Or if the display of a symbol is for the purpose of news or current affairs reporting by a 'person working in a professional journalistic capacity' 'in the public interest'.[593] As noted above, to rely on any of these exceptions a person would have to discharge the evidential burden in the same way that a journalist relying on the 'journalist defence' in Part 5.6 would have to.

9.69 The 'public interests' contemplated by the *Hate Symbols Act* pertain to 'religious, academic, educational, artistic, literary or scientific purposes' and 'news or current affairs'. There are some situations in which a prohibited symbol might be used in any of these contexts and in a way that caused limited or no harm of the type contemplated by the offence.

9.70 In contrast, if the recommendations in this report are accepted, the secrecy offences in Part 5.6 of the *Criminal Code* will all require proof of harm or likely harm – except for the deemed harm offence for officials in s 122.1, which, as modified by **Recommendations 1–3**, will be limited to a type of information that, if disclosed, will always or almost always cause harm. If **Recommendations 1- 4, 6, 8** and **12** are not accepted and the offences remain so broad as to encompass conduct which may cause little or no harm then the argument for a more general public interest defence is much stronger.

9.71 However, if the recommendations are accepted a general public interest test would only ever arise in the context of a Part 5.6 secrecy offence in circumstances where there was harm or likely harm to an essential national interest from the disclosure of the specific information in question. In most instances there will also be a form of harm caused by a breach of trust or duty by an official with access to sensitive intelligence, military or law enforcement information. The public interest to be weighed against these types of harms in an exception is likely to be more complex than those described in the *Hate Symbols Act*. The existing defence for journalists operates in a similar way to the exception for journalists in the *Hate Symbols Act*. Religious, academic, educational, artistic, literary or scientific purposes will rarely be public interest grounds for making a disclosure of the type of material covered by an updated Part 5.6.

9.72 Taking account of all these differences, the *Hate Symbols Act* is not a direct model for reframing the secrecy offences in Part 5.6 to include a more general public interest exception.

---

592 *Criminal Code* (n 532) s 80.2H(1)(c). Similar provisions apply to the offence for display of prohibited terrorist symbols: see *Criminal Code* (n 532) s 80.2HA(1)(c).

593 *Criminal Code* (n 532) s 80.2H(9).

However, there might be some merit in considering highlighting the public interest in news reporting by transforming the current journalism defence into an exception in a similar way to the *Hate Symbols Act*. This is discussed further below.

Recommendation on general public interest defence or element

9.73 Several non-government organisations made strong arguments as to why a general public interest test should be added as an *element* of disclosure offences and/or that a general public interest *defence* be added, including for officials. The proposed new measure(s) would be wider than those suggested in the *Hate Symbols Act* model. They would also be in addition to the existing journalist defence and the requirement that CDPP consider the public interest before commencing a prosecution and be separate to the protections available under schemes such as the *Public Interest Disclosure Act 2013* (Cth) (*PID Act*).

9.74 I do understand the attractions of such proposals. However, they would be complex and uncertain in practice. There are likely to be many competing public interests at play, some of which may shift over time. The inherent uncertainty of this type of general defence or element would make it very difficult to predict its outcome in advance. That lack of certainty has rule of law implications, as well as affecting the deterrence provided by the secrecy offences. This of course does not preclude 'public interest' continuing to be taken into account as a mitigating factor in sentencing.[594]

9.75 A general public interest element or a defence that applied to officials would also undermine the parliamentary intention that there be specific statutory mechanisms for providing immunity to those officials who bring forward wrongdoing (for example, in the form of the *PID Act* and the *National Anti-Corruption Commission Act 2022* (Cth)). It has been acknowledged that the *PID Act* requires reform, and that process is currently underway. If that process leads to a scheme that is easy to navigate and provides appropriate protections for those who wish to identify wrongdoing, a public interest element or a general public interest defence for officials in secrecy offences is not required for such disclosures. Concerns about 'dealing with' information by journalists, lawyers and civil society groups will be dealt with by **Recommendation 8**.

---

594 In the recent case of *R v McBride (No 4)* [2024] ACTSC 147 the sentencing judge noted that the deterrence aspect of sentencing can be lessened where a disclosure is made that is recognised as in the public interest or in circumstances where legitimate means of addressing the matters of concern were not available. His Honour noted that no attempt was made in the sentencing proceedings in that case either to establish that Mr McBride's thefts or disclosures were somehow in the public interest or that the legitimate and lawful means by which Mr McBride could have raised his concerns were inadequate ([232]).

RECOMMENDATION 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 defence for journalists as an exception rather than a defence.

Framing as an exception rather than a defence

9.76 Even though I have not recommended introducing a general public interest defence or altering the substance of the current journalist offence (subject to other recommendations being accepted), there is one other related issue worth considering: reframing the existing defence as an exception. This type of change would not materially alter the operation of the provision; nevertheless, some submitters suggested it would have merit.

9.77 At the public hearing HRLC said:

> there is an important, significant symbolic and principled difference in that you're excluding journalistic conduct from the ambit of the offence rather than including it and then providing for a defence. And while I appreciate the symbolic difference, [it] may not be material in a prosecution, although I'll come to that point in a moment, I do think it is really important that we are clear that journalism is not a crime, and that the conduct of public interest journalism that is otherwise potentially captured in these offences shouldn't be avoided by way of defence, but should be avoided by way of exclusion or exemption.[595]

9.78 Dr Keiran Hardy made a similar submission:

> I do think that even if it's symbolic in the law, the idea that this offence does not apply to people in these categories, is a preferable starting point to give greater confidence and trust, say, particularly for journalists, when we're talking about a chilling effect and whether they might, you know, be reluctant to report in the public interest and so on, that the offence actually saying 'this offence does not apply to you' is preferable to saying this is the offence and you're under it. But if you can raise an evidential burden in the courtroom, then you might be able to seek the defence for it. So I think while you know, in practical terms, there might not be a huge difference between them, I think symbolically and in terms of trust and potential chilling effect on journalists and something like that, an exception to the rule would be much more preferable in this case.[596]

595 Mr Kieran Pender, HRLC, *Public hearing transcript*, 25 March 2024, 23.
596 Dr Keiran Hardy, Griffith University, *Public hearing transcript*, 25 March 2024, 52.

9.79 Dr Dalla-Pozza suggested that it may provide greater clarity to cast the matter as an exemption rather than a defence:

> That exception, particularly with a similar exception to the one that was put in the Hate Crimes Act, actually makes the law clearer on the page. So if you're reading the legislation, as maybe we all should more often, you get a sense of what conduct the Parliament has decided to say is beyond the pale by doing an exception rather than relying on a defence. It's just easier, I think, for the ordinary lay person, should they read the legislation, to have a better sense of what harm the Parliament is trying to prevent. And so it goes back to our initial opening statement about the importance of the law being as clear as it can be for ordinary people, should they choose to read it, to be able to get a sense of what it is the Parliament is prescribing.[597]

9.80 At the public hearing, media organisations were not enthused by the idea of simply changing the existing journalist defence to an exception. Understandably, they were more focused on arguing for a broader public interest defence (or element) and removing the evidential burden from journalists.[598]

9.81 A defendant who wishes to rely on any exception or exemption provided by the law creating an offence bears the same evidential burden in relation to that matter as if it were a defence.[599] Thus simply recasting the defence as an exemption will not alter the evidential burden.

9.82 ARTK suggested one advantage of having journalism as an exception rather than a defence is that it may alter how police investigate, on the basis that they do not need to think about defences until the very end of an investigation.[600] However, I accept AFP's evidence that recasting the defence as an exemption will not alter the way police investigate a matter:

> in terms of the proposition of a carve out versus defence, an investigation would still look for any evidence that there is a defence available. We are would not want to continue with investigations if there's a clear defence available to the situation.
>
> If there was an exception in play or a defence in play, that would be an objective of the investigation … right from the beginning.[601]

9.83 There may be some merit in recasting the current journalism defence as an exception if this can be done without unnecessarily complicating the drafting. As HRLC and Dr Hardy

---

597 Dr Dominique Dalla-Pozza, Australian National University, *Public hearing transcript*, 25 March 2024, 53.

598 See Ms Georgia-Kate Schubert, ARTK, *Public hearing transcript*, 26 March 2024, 127–8; Mr Robert Todd, ARTK, *Public hearing transcript,* 26 March 2024, 128; Ms Phyllida Behm, AJF, *Public hearing transcript,* 26 March 2024, 129; Mr Peter Greste, AJF, *Public hearing transcript*, 26 March 2024, 129.

599 *Criminal Code* (n 532) s 13.3(3).

600 ARTK, *Submission 12*, 8–9.

601 Mr Stephen Nutt, Acting Assistant Commissioner, AFP, *Public hearing transcript*, 25 March 2024, 97–8.

suggested, the main benefit would be to convey that public interest journalism is not a crime. However, given that the change would be largely symbolic and media organisations were not initially enamoured of the idea, this proposed change should be subject to further consultation. The more impactful changes from this review as far as journalists are concerned are **Recommendation 8** – removing 'dealing with' offences – and **Recommendation 1** and **12** – removing deemed harm from the non-officials offences. If these are implemented it may remove any need to recast the current defence for journalists.

How 'journalist' is defined

9.84 Although this report has been using the shorthand 'journalist defence', the defence actually applies to any person who is 'engaged in the business of reporting news, presenting current affairs or expressing editorial or other content in news media'. This is broader than just journalists, and it would cover the many editorial, technical, administrative and legal staff who also work in these businesses.[602] Being engaged in a 'business' would cover self-employed or freelance journalists. It is arguable that those who provide content such as 'op eds' to news media businesses without themselves receiving remuneration are also engaged in the business of expressing editorial content in news media, though this is less clear. The recent *Hate Symbols Act* takes a similarly broad view, describing someone engaged in a 'journalistic capacity' as a 'journalist, editor, producer or other person involved in the process of making news reports or current affairs reports',[603] but the exceptions and defences in that Act apply to persons 'working in a *professional* journalistic capacity' (emphasis added) which may imply that receiving payment is required.

9.85 The only point at which the term 'journalist' is actually used is in the defence in s 122.5(6) is in relation to the specific defence for administrative staff who act under the direction of a 'journalist'. The term 'journalist' is not defined for the purpose of that paragraph, but its meaning would take into account the context in which it appears, which in this case is the context of a defence for a staff member of an entity 'engaged in the business of reporting news, presenting current affairs or expressing editorial or other content in news media'.

9.86 The joint academic submission said that s 14Q of the *Evidence Act 1977* (Qld) provides a more comprehensive definition of 'journalist', while the *Evidence Act 1995* (Cth) has a concise definition that simply provides that a journalist is a person who is engaged and active in the

602 Also see Supplementary Explanatory Memorandum, *EFI Bill* (n 566) 96 [632].

603 *Counter-Terrorism Legislation Amendment (Prohibited Hate Symbols and Other Measures) Act 2023 (Cth)* sch 1 item 7.

publication of news.[604] AJF supported adopting the Queensland model.[605] In contrast, ARTK said that the current approach to the definition in Part 5.6 is broadly appropriate.[606]

9.87 In his evidence, the Director-General of Security said that 'foreign intelligence services use journalists cover and tradecraft, as in pretend to be a journalist to do their job'.[607] As MEAA noted, such people are not journalists and should not be given the protections afforded to journalists.[608] I did not take the Director-General's comments to suggest that the scope of the defence for journalists be altered. In any case, it is difficult to see that the journalist defence is likely to be relevant to a situation involving a foreign intelligence service, which is presumably more interested in covertly obtaining rather than communicating Australian Government information. The situation may be more complex for the espionage and foreign interference offences in Part 5.2.

9.88 It will ultimately be a question of fact whether a person falls into the relevant category. This is true for the current definition, as well as those under the Queensland and Commonwealth Evidence Acts. At this stage no compelling case has been made that there is a need to alter the current definition.

Application of the journalist defence beyond section 122.4A

9.89 There is one final matter to note on the journalist defence. As it is currently drafted, the defence applies to all of the offences in Part 5.6, not just the 'non-officials' offence in s 122.4A. Theoretically, a situation could arise where a person who was formerly a Commonwealth official and later became a journalist could communicate, contrary to s 122.1 or s 122.2, 'inherently harmful information' or information that would 'cause harm to Australia's interests' that they remembered from their Commonwealth employment. If the communication of that information was in the course of the person's (new) capacity as a journalist and they reasonably believed that engaging in the conduct was in the public interest then theoretically they could rely on the defence in s 122.5(6) to defend against a prosecution for offences that apply to former officials. It seems unlikely that this was an intended operation of this defence. Consideration could be given to an amendment to ensure that a defence such as s 122.5(6), which is clearly directed at information that was not obtained by the defendant in the course of their employment with the Commonwealth, can only apply to the s 122.4A offences for 'non-officials'.

604 Joint Academic Submission, *Submission 13*, 15–16.
605 AJF, *Submission 11*, [8.7]–[8.11].
606 ARTK, *Supplementary submission 21*, 9.
607 Mr Mike Burgess, Director-General of Security, ASIO, *Public hearing transcript,* 25 March 2024, 18.
608 Mr Paul Farrell, MEAA, *Public hearing transcript,* 26 March 2024, 126–7; MEAA, *Supplementary submission 22*, 4.

Other defences in section 122.5

9.90 Although the defence relating to journalists has received the most attention, there are a range of other defences in s 122.5. These are summarised below:

- Exercising a power, or performing a function or duty, in the person's capacity as a public official or a person who is otherwise engaged to perform work for a Commonwealth entity (s 122.5(1)(a)).
- Communicating, removing, holding or otherwise dealing with the information in accordance with an arrangement or agreement to which the Commonwealth or a Commonwealth entity is party and which allows for the exchange of information (s 122.5(1)(b)).
- The relevant information had already been communicated or made available to the public with the authority of the Commonwealth (s 122.5(2)).
- The person engaged in the offending conduct for the purpose of communicating the relevant information to specified integrity or oversight agencies (s 122.5(3)).
- The person engaged in the offending conduct for the purpose of communicating the relevant information in accordance with the *Public Interest Disclosure Act 2013* or the *Freedom of Information Act 1982* (s 122.5(4)).
- The person engaged in the offending conduct for the primary purpose of reporting a criminal offence or maladministration to an appropriate agency of the Commonwealth, a State or a Territory (s 122.5(4A)).
- The person engaged in the offending conduct for the purpose of communicating the relevant information to a court or tribunal (whether or not as a result of a requirement) (s 122.5(5)).
- The person engaged in the offending conduct for the primary purpose of obtaining or providing, in good faith, legal advice in relation to an offence against Part 5.6 or the application of any right, privilege, immunity or defence (whether or not in Part 5.6) in relation to such an offence (s 122.5(5A)).
- The information has already been communicated, or made available, to the public (does not apply to information they made or obtained as an official, contractor or under an agreement or where they were involved in the prior publication) and:
  - at the time of the communication, removal, holding or dealing, the person believes that engaging in that conduct will not cause harm to Australia's interests or the security or defence of Australia, and
  - having regard to the nature, extent and place of the prior publication, the person has reasonable grounds for that belief (s 122.5(8)).
- The person did not obtain the information as an official, contractor or under an agreement and reasonably believes that the making or obtaining of the information

by the person was required or authorised by law, but only where one of the following also applies:

- the person communicates the information to the person to whom the information relates
- the person is the person to whom the information relates
- the communication, removal, holding or dealing is in accordance with the express or implied consent of the person to whom the information relates (s 122.5(9)).

9.91 Submissions were made or minor issues identified with some of these defences. These are discussed below.

Without lawful authority – section 122.5(1)

9.92 The Law Council of Australia said that it was unusual that whether an action was undertaken with lawful authority is expressed as a defence not an exception to the offences:

> [It is] unusual that an offence provision would, other than for the operation of the defence in section 122.5(1), criminalise a vast range of innocuous and every-day transactions comprising the working of government. This is unusual because it inverts the usual structure of a criminal offence, inclusion of an offence-specific defence is a departure from the general principle that a defendant is presumed to be innocent, and the prosecution must prove the matters essential to establishing the criminality of conduct. As stated above, offence provisions should not be so broadly drafted that they inadvertently capture a wide range of benign conduct, and rely on defences, subject to a reversal of the evidential burden, to determine what is actually proscribed.[609]

9.93 The Law Council of Australia noted that the secrecy offences contained in the *Official Secrets Act 1989* (UK) proscribe disclosures that occur 'without lawful authority' and supported such an approach being followed in the *Criminal Code*.[610] A similar approach is taken to the secrecy offences in the *Intelligence Services Act 2001* (Cth) and the *Australian Security Intelligence Organisation Act 1979* (Cth) (*ASIO Act*), which refer to disclosures made without the authority of the agency head or another specified official.

9.94 Ultimately, this is a matter of drafting style. As noted in the discussion above about the journalist defence versus exception, it would not alter the evidential burden.

The defence in section 122.5(4) and the Archives Act 1983

9.95 Section 122.5(4) contains a defence to a prosecution under Part 5.6 if the person communicated the relevant information, or removed, held or otherwise dealt with it for the

609 Law Council of Australia, *Submission 19*, 40 [140].
610 Law Council of Australia, *Submission 19*, 40 [142].

purpose of communicating it, in accordance with the *PID Act* or the *Freedom of Information Act 1982* (Cth) (*FOI Act)*. Another piece of legislation that provides a right of access to documents held by the Australian government and agencies is the *Archives Act 1983* (Cth).

9.96 As the National Archives of Australia noted in its submission to this review:

> The access decision-making process undertaken by officers of National Archives is similar to the access decision-making process undertaken by agency officers when dealing with requests for access to documents of those agencies under the *Freedom of Information Act 1982*.[611]

9.97 The National Archives also said, and I accept, that is it usual that officers communicate, move or copy records for the purpose of making decisions and disclosures.[612] This may bring those actions within the defence in s 122.5(1), but the same could be said for people who deal with information for *FOI Act* or *PID Act* purposes. To avoid any uncertainty about the interaction between the *Archives Act* and the offences in Part 5.6, it may be beneficial to consider amending the defence in s 122.5(4) to include the *Archives Act*.

Defence for lawyers – section 122.5(5A)

9.98 The defence for lawyers in s 122.5(5A) only applies to the provision of legal advice in relation to offences under Part 5.6. This means that presently a lawyer who receives, in good faith, information from a client they are assisting with another matter may commit an offence. This is most likely to occur in relation to the 'dealing with' offences. For example, a lawyer engaged to assist a person with a family law dispute might be told things by their client that are 'classified information' or go to the 'operations or sources used by a law enforcement agency'. The information might be directly relevant to say, a child custody dispute. At the moment the lawyer would likely commit an offence when they receive the information and a further offence if they make a note of the effect of the information. It seems to be an unreasonable burden on the role of lawyers acting in good faith as part of our legal system for the defence to not be available in these circumstances.

9.99 The Law Council of Australia made a similar point and suggested that s 35P(3)(b) and (e) of the *ASIO Act* provides a better model. The Law Council also noted that a former INSLM made recommendations in *The operation of Part 3, Division 1 of the National Security Information (Criminal and Civil Proceedings) Act 2004 as it applies in the Alan Johns matter* report to

611 National Archives of Australia, *Submission 24.*
612 National Archives of Australia, *Submission 24.*

ensure effective legal representation.[613] It is not sufficient protection for lawyers or the legal system that agencies have policies applying to Commonwealth officials that require them to only use 'cleared lawyers'.[614]

9.100 The Law Council recommended that the defence be broadened so that:

> Section 122.5 should include an exception for where the conduct (i.e., communication/dealing) is engaged in for the purpose of obtaining or providing legal advice in relation to the matter the subject of the offence.
>
> Section 122.5 should include an exception that offence provisions do not apply if the disclosure was for the purposes of any legal proceedings arising out of, or otherwise related to, the Division or of any report of any such proceedings.[615]

9.101 The concerns identified by the Law Council would seem to be largely resolved by **Recommendation 8** (removing the 'dealing with' offences for non-officials) and **Recommendation 12** (ensuring offences for non-officials require evidence of harm). If those recommendations are not accepted then the amendments to the defence for lawyers that the Law Council proposed should be made.

The defence of prior communication – section 122.5(8)

9.102 The defence that 'information that has previously been communicated' in s 122.5(8) requires that at 'the time of the communication, removal, holding or dealing, the person believes that engaging in that conduct will not cause harm to Australia's interests or the security or defence of Australia'. This definition includes both the defined term 'cause harm to Australia's interests' and the defined term 'security or defence of Australia'. This is unnecessary, as the current definition of 'cause harm to Australia's interests' already expressly includes harm or prejudice to what is defined as the 'security or defence of Australia'.

9.103 If the definition of 'cause harm to Australia's interests' is modified as proposed by **Recommendation 6**, the defined phrase 'security or defence of Australia' will become redundant and should be removed from the definitions section and the defence in s 122.5(8). Otherwise, those terms should be given the meanings proposed in **Chapter 5**.

---

613 Law Council of Australia, *Submission 19*, 45-46 [161]–[165]; Grant Donaldson, INSLM (former), *The Operation of Part 3, Division 1 of the National Security Information (Criminal and Civil Proceedings) Act 2004 as it Applies in the Alan Johns Matter* (Report, 17 June 2022).

614 See comments by Dr David Neal SC and Mr Philip Boulten SC, Law Council of Australia, *Public hearing transcript,* 26 March 2024, 172–3 in references to Office of National Intelligence, *Submission 8*, 13.

615 Law Council of Australia, *Submission 19*, 46, recommendation 22.

Removed held or otherwise dealt with – section 122.5(11)

9.104 Several of the defences use the phrase 'the person communicated, removed, held or otherwise dealt with the information'. Presumably the use of the word 'otherwise' is meant to differentiate communicating, removing and holding from the dealing with part of this expression, although it isn't clear if the intent is to limit the defence so it cannot apply to 'dealing with' that is also communicating, holding or removing.[616] As discussed in **Chapter 6** the definition of 'deal' is somewhat confusing and currently includes communicating. It also includes categories such as 'possess' that could overlap with the ordinary meaning of 'holding'. It may be beneficial to review the wording used in defences, particularly in light of **Recommendation 7** (refining dealing) and **Recommendation 9** (proper place of custody).

616 Section 122.5(11) provides that for some defences 'it is not necessary to prove that information, that was removed, held or otherwise dealt with for the purpose of communicating it, was actually communicated'.

Chapter 10: Safeguards for individual rights and policies that directly affect investigations and prosecutions

10.1 INSLM reviews must have regard to whether the legislation being reviewed contains appropriate safeguards for protecting the rights of individuals.[617] I must also consider the operation and effectiveness of the law, which necessarily involves consideration of the way that the law is operating in practice. In combination, this allows consideration of safeguards in Part 5.6 of the *Criminal Code* itself and safeguards in directions made under other laws that are directly relevant, as well as relevant policies.

10.2 This chapter looks at the following safeguards in Part 5.6:

- the requirement that the Attorney-General's written consent be obtained before a prosecution is instituted (s 123.5(1)(a))
- for prosecutions that relate to 'security classified information', the requirement that the Attorney-General certify that at the time of the conduct that is alleged to constitute the offence, it was appropriate that the information had a security classification (s 123.5(1)(b)).

10.3 It also looks at the following directions and policies:

- a Ministerial Direction given under s 37(2) of the *Australian Federal Police Act 1979* (Cth) by the Attorney-General in relation to the investigation of journalists[618]
- the Prosecution Policy of the Commonwealth
- the Australian Federal Police (AFP) Operational Prioritisation Model
- The AFP National Guideline on Sensitive Investigations.

10.4 The defences available under s 122.5, which might also be described as safeguards, were discussed in **Chapter 9**.

617 *Independent National Security Legislation Monitor Act 2010* (Cth) ss 6, 8 ('*INSLM Act*').

618 Attorney-General (Cth), *Ministerial Direction (Australian Federal Police): Australian Federal Police Act 1979*, 20 October 2023.

Attorney-General's consent before prosecution

10.5 Before proceedings are instituted to commit a person to trial for an offence under Part 5.6, the written consent of the Attorney-General is required.[619] However, a person may be arrested, charged and remanded in custody or on bail without consent having been obtained.[620] In deciding whether to consent, the Attorney-General must consider whether there may be an applicable defence.[621] No other specific considerations are listed in the Act, leaving the Attorney-General a wide discretion as to both the matters that the Attorney-General may consider and the ultimate decision whether to consent.

10.6 The requirement to obtain consent to prosecute is a frequent and longstanding requirement for offences that may have significant international relations and national security implications.[622] Similar consent requirements are contained in the secrecy offences in the *Australian Security Intelligence Organisation Act 1979* (Cth), *Intelligence Services Act 2001* (Cth) (*IS Act*) and *Office of National Intelligence Act 2018* (Cth). The *Criminal Code* also contains a number of non-secrecy offences relating to Australia's international relations or national security that require the Attorney-General's consent.[623] There are similar consent requirements in the United Kingdom, Canada and New Zealand.[624]

10.7 Through a direction given to the Commonwealth Director of Public Prosecutions (CDPP), the requirement to obtain the Attorney-General's consent has been extended to proceedings for the prosecution of a journalist under certain other Acts.[625] On 21 November 2023, the Attorney-General announced the government's intention to require ministerial consent to

---

619 *Criminal Code Act 1995* (Cth) s 123.5(1)(a) ('*Criminal Code*').

620 *Criminal Code* (n 619) s 123.5(2*).* No further steps in proceedings may be taken without consent being obtained.

621 *Criminal Code* (n 619) s 123.5(4).

622 Attorney-General's Department (AGD), *Submission 7*, 22 [101].

623 *Criminal Code* (n 619) ss 16.1, 82.13, 83.5, 93.1, 115.6, 123.5, 268.121, 270.3B, 490.6.

624 The *Official Secrets Act 1989* (UK) requires the consent of the Attorney-General, including where the disclosure concerns intelligence, defence or international relations. The consent of the Attorney-General is not required if the prosecution concerns disclosures about police powers. Attorney-General consent is also required for certain secrecy prosecutions in Canada and New Zealand. See for example, *Security of Information Act, RSC 1985, c O-5,* s 24 (Canada) and *Crimes Act 1961* s 78B (NZ).

625 Attorney-General (Cth), *Ministerial Direction (Commonwealth Director of Public Prosecutions): Director of Public Prosecutions Act 1983*, 30 September 2019: this direction was issued under subsection 8(1). The relevant offences were s 35P of the *Australian Security Intelligence Organisation Act 1979* (Cth) ('*ASIO Act*'); ss 3ZZHA, 15HK, 15HL and 70 of the *Crimes Act 1914* (Cth) ('*Crimes Act*'); ss 131.1 and 132.1 of the *Criminal Code* (n 619); and s 73A of the *Defence Act 1903* (Cth).

prosecute a journalist for other secrecy offences. The Attorney-General's Department (AGD) indicated that this is to be done through legislation.[626]

What is the purpose of requiring consent?

10.8 AGD explained the policy behind the requirement:

> [The consent requirement] enables the Attorney-General to have regard to considerations that are particularly within the responsibility and knowledge of the executive government, such as Australia's international relations or national security, in determining whether a prosecution should proceed.[627]

10.9 The Revised Explanatory Memorandum to the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2018 (EFI Bill) also described the requirement as promoting the right in art 9(1) of the *International Covenant on Civil and Political Rights* (right to liberty and freedom from arbitrary detention) by requiring the Attorney-General to 'consider whether the conduct was authorised and therefore whether the accused has a defence available'.[628]

10.10 AGD, AFP and CDPP advised me that matters are only put to the Attorney-General seeking consent *after* AFP has provided a brief of evidence to CDPP and CDPP has made an independent decision that prosecution is appropriate in accordance with the Prosecution Policy of the Commonwealth, including the application of the public interest test in that policy (the Prosecution Policy of the Commonwealth is discussed further below.)

10.11 Therefore, as the Law Council of Australia noted, the consent requirement 'is intended to be a safeguard to benefit the offender as the Attorney-General will only be able to prevent prosecutions advancing beyond committal by refraining from providing consent'.[629]

Submission on whether consent by the Attorney-General is appropriate

10.12 Most civil society and media organisations who made submissions agreed that, while not a perfect safeguard, the consent requirement is at least a pragmatic safeguard and should be retained.[630] For example, the Human Rights Law Centre (HRLC) said that the consent

---

626 Attorney-General (Cth), 'Reforms to Commonwealth Secrecy Offences' (Media Release, 21 November 2023); AGD, *Submission 7*, 4 [11].

627 AGD, *Submission* 7, 22 [101].

628 Revised Explanatory Memorandum, National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2018 ('*EFI Bill*') 9 [26].

629 Law Council of Australia, *Submission 19*, 46 [168].

630 Media, Entertainment and Arts Alliance (MEAA), *Submission 9*, 7; Australian Human Rights Commission (AHRC), *Submission 17*, 25–26; Human Rights Law Centre (HRLC), *Submission 14*, 15.

requirement 'is not preferable as a matter of principle, but in the absence of strong protections such as a general public interest defence, is necessary in practice'.[631]

10.13 The Australian Human Rights Commission (AHRC) expressed some concern that the 'discretion [to prosecute] rests within the executive arm of government and introduces a political element to prosecutions', although it concluded that the requirement for Attorney-General consent should be retained, as it does provide a safeguard against inappropriate prosecutions.[632] The Media, Entertainment and Arts Alliance (MEAA) and the Law Council also acknowledged and cautioned against the risk of politicisation. However, on balance, they preferred that the consent requirement be retained.[633]

10.14 In contrast, the Alliance for Journalists' Freedom (AJF) submitted that the consent requirement should be removed because, rather than being an effective safeguard, it 'arguably risks making the decision to prosecute a journalist a political matter and exposes the Attorney-General to allegations of political bias':[634]

> The AJF recognises the Attorney-General's position as the First Law Officer, and accepts that, in this role, they are to uphold the rule of law and the integrity of the courts. But the Attorney-General is also a politician. To ask the Attorney-General to consent to the prosecutions under Part 5.6 risks creating actual or perceived conflicts of interest.[635]

10.15 At the public hearing AJF elaborated that, regardless of whether an 'Attorney-General decides to consent to a prosecution or issues a directive to withdraw from a prosecution, that decision is going to be seen as political in nature'.[636] AJF noted, for example, that the Attorney-General may be in a position to decide whether to consent to the prosecution of a journalist who has written a story about the Attorney-General or their government.[637]

Retain consent requirement

10.16 I acknowledge the concern that there may be at least a perception of politicisation of a decision to prosecute a person for a secrecy offence, particularly a decision to prosecute a journalist – or one journalist but not another. However, the fact that the Attorney-General's consent is sought only *after* the CDPP makes an independent decision to proceed with a

631 HRLC, *Submission 14*, 15.
632 AHRC, *Submission 17,* 25 [103].
633 MEAA *Submission 9*, 7; Law Council of Australia, *Submission 19*, 46.
634 Alliance for Journalists' Freedom (AJF), *Submission 11*, [7.1].
635 AJF, *Submission 11*, [7.1].
636 Mr Peter Greste, AJF, *Public hearing transcript*, 26 March 2024, 132.
637 There are provisions in the *Acts Interpretation Act 1901* (Cth) that can be used to allow another portfolio Minister or a different Minster or a member of the Executive Council to act on behalf of a Minister, including where there is a conflict of interest: ss 19, 34AAB. However, the existence of these provisions is unlikely to resolve AJF's concern.

prosecution provides some mitigation to this perception and means that the consent requirement can only be used to benefit an accused person.

10.17 I consider it appropriate that the requirement to seek the Attorney-General's consent for the secrecy offences in Part 5.6 be retained. In a prosecution for an offence relating intelligence information, national security, defence and/or international relations or sensitive law enforcement capabilities, there are many factors that are particularly within the responsibility and knowledge of the executive government that it is proper for the Attorney-General to take into account. These include Australia's international relations; and balancing the risk of additional sensitive information being exposed during proceedings with the desirability of continuing a prosecution.

10.18 As the First Law Officer, the Attorney-General is also well placed to consider broader public interest considerations that may arise in the prosecution of a secrecy offence, particularly where whistleblowers or journalists are involved. Even if the CDPP has already considered these matters, it is appropriate that the requirement for Attorney-General's consent be retained to provide a further safeguard in that respect.

Other proposals on the consent requirement

10.19 Having concluded that the requirement to obtain the Attorney-General's consent should be retained, it is now necessary to turn to submissions that recommended some variation to the current consent arrangements.

Listing public interest factors

10.20 The first issue is whether there should be a more extensive list of matters that the Attorney-General is required to have regard to in deciding whether to consent. Australia's Right to Know (ARTK) suggested that the Attorney-General be required to consider the public interest in communicating facts and opinions to the public by news media and the ability of the media to access sources of facts.[638] Conversely, AGD submitted that it 'did … not consider it necessary or appropriate to require that the Attorney-General must have regard to any other matters'.[639] When considering a related issue in the AGD *Review of Secrecy Provisions*, AGD noted that even a non-exhaustive list of public interest factors could potentially constrain what is interpreted as a public interest factor and that it was important that the public

638 Australia's Right to Know (ARTK), *Submission 12*, 19 [99].

639 AGD, *Submission 7*, 22 [104]. In accordance with s 123.5(4), the Attorney-General must have regard to whether the conduct might be authorised in a way mentioned in s 122.5 (defences).

interest be able to adapt over time.[640] A similar argument can be made about the factors that it is appropriate for the Attorney-General to have regard to.

10.21 Having regard to the nature of the decision whether to consent to a prosecution, and its intended role as a final safeguard to allow the Attorney-General to take into account matters within the special knowledge of the executive, the factors that the Attorney-General may have regard to are broad. If some factors were to be listed, this would need to be an open-ended list in order to still provide appropriate discretion, and it would still ultimately be up to the Attorney-General to weigh both the listed and any relevant unlisted factors to reach a decision. Furthermore, the relevant factors will depend on the particular circumstances of the case and may change over time. On balance I do not see significant benefit in adding a list of factors that the Attorney-General must have regard to.

Time limit

10.22 A second issue that was raised is whether there should be a time limit for the Attorney-General to make a decision on providing or withholding consent. The primary concern is that a person under investigation may not know for a long time whether they will be prosecuted and that this can cause significant hardship, as well as risks of degradation of evidence with the passage of time.[641] Following some discussion of this issue at the public hearing, ARTK helpfully provided a detailed supplementary submission setting out their proposal. In MEAA's supplementary submission it agreed that a time limit should be introduced.[642]

10.23 The key elements of the ARTK proposal are that:

- CDPP would be under a statutory duty to serve notice on the defendant and the Attorney-General, which indicates an intention to prosecute.
- A statutory time frame for the Attorney-General's consideration would run from the date of that notice (60 days was suggested).
- At the expiry of the time period, a decision to refuse consent to prosecute would be deemed to be made by law. From that point in time, the Attorney-General is *functus officio* – that is, incapable of exercising the power to consent to prosecute unless and until CDPP issues a new notice.
- Any decision to prosecute made within the 60-day period would not be subject to merits review under the *Administrative Appeals Tribunal Act 1975* (Cth) but would be reviewable under the *Administrative Decisions (Judicial Review) Act 1977* (Cth) (*ADJR Act*) and would be subject to a statutory right to reasons under that Act.

640 AGD, *Review of Secrecy Provisions* (Final Report, 21 November 2023) 48 [217] ('*AGD Review of Secrecy Provisions*').
641 ARTK, *Submission 12*, 19 [95].
642 MEAA, *Supplementary submission 22*, 5.

- If a deemed or actual decision not to prosecute is made and then significant fresh and compelling material that was not reasonably available at the time of the initial notice comes to light, CDPP could issue a further notice of intention to prosecute. Time would run in the normal manner from the issue of that second notice. Whether there is or is not significant fresh and compelling material that was not reasonably available at the time of the initial notice would be a matter which could be reviewed as objective jurisdictional facts under the *ADJR Act*. There would also be a statutory right to reasons from any CDPP decision to issue a new notice.[643]

10.24 I have no doubt that it would be extremely stressful for a person who is being investigated for a secrecy offence, or any other offence, to not know for a long period whether they were going to be prosecuted. I also accept that many police investigations, including those for secrecy offences, can take a long time. That may be for a range of factors, including resources, complexity and the need to obtain evidence from people or organisations outside Australia. The addition of a requirement to obtain the Attorney-General's consent (and in some cases certification) can certainly add to that time. There have been cases where it has appeared that a prosecution was effectively 'on hold' for an extended period while the matter sat with an Attorney-General.

10.25 It is incumbent on any Minister, including the Attorney-General, to discharge a statutory decision-making function in a timely manner.[644] Theoretically, if the Attorney-General has not made a decision within a reasonable time, under s 75(v) of the Constitution a writ of mandamus could be sought to require the Attorney-General to make a decision. This would depend on whether the Attorney-General could be considered to have a duty to decide whether to consent to a prosecution, enforceable by way of mandamus. Further, what amounts to a reasonable time would ultimately be for a court to determine, having regard to the circumstances of the particular case within the context of the decision-making framework established by the Act. This avenue is likely to provide limited assistance and only in cases of lengthy, unexplained delays. A person who has been arrested, charged or remanded could also seek to have a proceeding discontinued because of unreasonable delay.[645] Section 123.5(3) expressly provides that nothing in the consent provision prevents the discharge of the accused if proceedings are not continued within a reasonable time.

---

643 ARTK, *Supplementary submission 21*, 10–11. Where a prosecution required the Attorney-General's certification in respect of security classified information, as well as consent to the prosecution, it is likely that the same temporal concerns would arise. I have therefore assumed that the ARTK proposal would apply to both elements of the Attorney-General's decision in such a case.

644 *Tickner v Bropho* (1993) 40 FCR 183; *Plaintiff S297/2013 v Minister for Immigration and Border Protection* (2014) 255 CLR 179, [37].

645 The procedural rules of the relevant jurisdiction will also be relevant. Some include clear time limits.

10.26 Further, as noted in the Revised Explanatory Memorandum:

> Australian common law recognises that a prosecution may be stayed where there is undue delay, to protect Australia's justice system from abuse of processes. The right to stay a prosecution also supports the Court's role in providing procedural fairness to a defendant, and helps maintain public confidence in the administration of justice.[646]

10.27 That said, the discretionary power to stay proceedings is exercised only in 'exceptional circumstances and as a last resort'.[647]

10.28 A statutory obligation to decide to grant or withhold consent within a set period such as that proposed by ARTK would bring some certainty. However, adding this type of requirement goes beyond the existing judicial discretion to stay proceedings in cases of undue delay. It would be a significant change to the current law and one without precedent in other Commonwealth offences that require the Attorney-General's consent.

10.29 A requirement to consent within 60 days is not without risk. The most obvious one is that it may deprive the Attorney-General of proper opportunity to ask the relevant agencies to gather and provide additional information which he or she considers relevant to weighing the merits of deciding to consent or not. The same can be said for a decision to certify whether information was classified correctly, which in some cases may involve a large volume of information.[648] The proposal that CDPP be able to issue a new notice if there is fresh and compelling evidence would not resolve this – it may be that the additional information that the Attorney-General requests does not reach that legal threshold, but it could still be information relevant to proper consideration of the matter. In my view, this concern makes the proposal, as presented, unworkable. I also note that making a decision involving intelligence agency information subject to the *ADJR Act* is inconsistent with the longstanding exemption of most decisions relating to those agencies from that Act.[649]

Consent to summary proceedings

10.30 A third issue that was raised is whether the requirement to obtain the Attorney-General's consent should be extended to prosecutions that proceed summarily. Section 4J of the *Crimes Act 1914* (Cth) has the effect of permitting any offence that carries a penalty of 10 years or less (which includes those in Part 5.6) to be dealt with summarily with the consent of the

646 Revised Explanatory Memorandum, *EFI Bill* (n 628) 156 [662].
647 *GLJ v The Trustees of the Roman Catholic Church for the Diocese of Lismore* [2023] HCA 32.
648 AFP, *Submission 18*, 8.
649 *Administrative Decisions (Judicial Review) Act 1977* (Cth) ('*ADJR Act*') s 3(1) definition of 'decision to which this Act applies' and sch 1.

prosecutor and the defendant. The practical effect is that the trial would be judge-only and that the maximum penalty is reduced.[650]

10.31 The Law Council and ARTK both identified that s 123.5 only applies to 'proceedings for the commitment of a person to trial'. Therefore, it does not apply to prosecutions for offences under Part 5.6 that are dealt with summarily. For those prosecutions, there will be no committal hearing and no indictment. They therefore proposed that s 123.5 should extend to summary prosecutions, as even they may have significant impact on freedom of expression and media freedoms.[651]

10.32 In contrast, the equivalent consent provision in the *IS Act* requires the Attorney-General's consent for 'a prosecution under this Division' being 'instituted', and similar wording is used in the direction to CDPP to obtain consent in certain other secrecy-related prosecutions.[652] This would cover both prosecutions on indictments and prosecutions that proceed summarily.

10.33 The factors peculiarly within the knowledge of the Executive that make it reasonable for the consent requirement to be retained apply equally to any prosecution under Part 5.6, whether it is prosecuted by indictment or summarily. The fact that an individual must agree to a proceeding being dealt with summarily does not remove the need for the Attorney-General to be able to consider these broader public interest matters before a prosecution progresses. Furthermore, a defendant should not be placed in a position of having to decide whether to consent to having a proceeding dealt with summarily, with the advantage of lower maximum penalties, at the cost of losing the safeguard of the Attorney-General's consent to the prosecution.

RECOMMENDATION 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.

10.34 A time limit should not be added to the consent requirement and a list of the factors that the Attorney-General must have regard to should not be set out in legislation.

650 *Crimes Act* (n 625) s 4J.

651 Law Council of Australia, *Submission 19*, 46 [169]; ARTK, *Submission 12*, 18 [94].

652 *Intelligence Services Act 2001* (Cth) ('*IS Act*') s 41A; Attorney-General (Cth), *Ministerial Direction (Commonwealth Director of Public Prosecutions): Director of Public Prosecutions Act 1983*, 30 September 2019.

Certification requirement

10.35 For prosecutions that relate to 'security classified information', the Attorney-General is also required to certify that 'at the time of the conduct that is alleged to constitute the offence, it was appropriate that the information had a security classification'.[653]

10.36 I have recommended that Part 5.6 should be amended so that offences no longer rely on a security classification applied under a policy as an element of a crime (**Recommendation 1**). If that recommendation is accepted then it will follow that provisions in the *Criminal Code* relating to certification should be repealed, as they will no longer be required. However, if that recommendation is not accepted, certification should be retained as a condition precedent to prosecution for any prosecution (whether on indictment or dealt with summarily).[654] It is not a perfect safeguard and its application will be complex, but if security classification is retained then it is essential, particularly given all of the problems with relying on classifications applied for administrative purposes in a criminal proceeding, as discussed in **Chapter 4**.

Ministerial Direction to AFP on journalists

10.37 The Attorney-General has given AFP a direction in relation to professional journalists and news media organisations. The current direction states:

> Regarding investigation of unauthorised disclosure of material made or obtained by a current or former Commonwealth officer involving a professional journalist or news media organisation [the Attorney-General expects] the AFP to take into account the importance of a free and open press in Australia's democratic society and to consider the broader public interest implications before considering investigative action involving a professional journalist or news media organisation.[655]

---

653 *Criminal Code* (n 619) s 123.5(1)(b). See also the discussion in Chapter 4 concerning reliance on a security classification as an element of an offence.

654 Note that certification does not have evidentiary value: AGD, *Submission 7*, 23, [106]. This is consistent with a recommendation from the Parliamentary Joint Committee on Intelligence and Security (PJCIS): PJCIS, Parliament of Australia, *Advisory Report on the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 (Report, June 2018)* 76 [3.169], recommendation 10. See also recommendation 11 and recommendation 12 of that report in relation to evidentiary certificates. As noted by AHRC, there would be significant rule of law and perhaps constitutional issues around the separation of powers if there was an attempt to amend the provision so that it operated as a conclusive certificate: Ms Lorraine Finlay, Human Rights Commissioner, AHRC, *Public hearing transcript*, 25 March 2024, 37.

655 Attorney-General (Cth), *Ministerial Direction (Australian Federal Police): Australian Federal Police Act 1979*, 20 October 2023.

10.38 This direction requires that AFP consider 'the importance of a free and open press in Australia's democratic society and to consider the broader public interest implications' every time it takes any 'investigative action'. This would include investigative actions such as seeking warrants or questioning a person. As discussed below, AFP has a 'sensitive investigations guideline' that, amongst other things, provides some oversight to ensure that this direction is adhered to.

10.39 At a practical level, this direction provides a significant safeguard against the investigation of journalists without a careful weighing of the public interest regularly throughout the investigative process. For this reason it should be retained. However, I also accept the submissions of AHRC and others that the direction does not provide great comfort given an Attorney-General could change it at any time and is therefore not equivalent to a legislated protection.[656]

10.40 As a minor technical matter, I note that the current direction refers to current and former 'Commonwealth officers', whereas the offences in Part 5.6 *also* apply to persons 'otherwise engaged to perform work for a Commonwealth entity' (**Chapter 1**). I am confident that AFP takes a broad view of the expectations that the Attorney-General articulates in the direction and would apply the direction equally to 'Commonwealth officers' and to persons 'otherwise engaged to perform work for the Commonwealth'. Nevertheless, a minor drafting adjustment should be considered next time the direction is reissued.

Australian Federal Police policies

10.41 In its submission AFP outlined a series of internal governance structures that are typically enlivened by referrals of alleged breaches and subsequent investigations of secrecy offences in Part 5.6. Again, these are not laws and can be changed at any time. A number of civil society and media groups said that they did not regard policies as 'safeguards' for this reason. Nevertheless, understanding them provides insight into how the offences in Part 5.6 are currently investigated and, therefore, how the laws are operating.

Operational Prioritisation Model

10.42 Following the *Review into the AFP's Response to and Management of Sensitive Investigations* by Mr John Lawler AM APM (Lawler Review), the AFP introduced a new 'Operational Prioritisation Model' (OPM) in 2023.[657] It is designed to inform operational, treatment and

656 AHRC, *Submission 17*, 18 [84].

657 John Lawler AM APM, *Review into the AFP's Response to and Management of Sensitive Investigations* (Report, 17 January 2020).

resource distribution decisions about crime referrals to ensure they are 'appropriately focused on ensuring public safety, minimising community harm and protecting national interests'.[658] It ultimately prioritises resources to 'high harm matters where the AFP can deliver the greatest impact' to eliminate or reduce the harm.[659]

10.43 The articulation and assessment of the harm or possible harm caused by an unauthorised disclosure is critical to the OPM. However, it bears noting that this internal appraisal is distinct from proving harm beyond reasonable doubt as an element of the offences.[660]

10.44 AFP advised that secrecy offences which would generally rate highly on AFP's OPM would involve:

- any misuse or unauthorised disclosure of material classified 'top secret', regardless of the number of records
- misuse or unauthorised disclosure of material classified 'secret' where 2 or more elements of s 122.3 of the *Criminal Code* are present
- misuse or unauthorised disclosure of material made or obtained by an intelligence agency where 2 or more elements of s 122.3 of the *Criminal Code* (that is, factors for the aggravated offence) are present, or
- misuse or unauthorised disclosure of material relating to the operations, capabilities, technologies, methods or sources of a law enforcement agency where 2 or more elements of s 122.3 of the *Criminal Code* are present.[661]

10.45 At the public hearing, AFP said that the 'harm' arising out of any offence is initially described by a referrer (i.e. a government agency) in a 'harm statement' that forms part of the 'Agency Report a Crime to the AFP form'.[662] That form asks:

> What is the Harm now and/or in the future to your agency / national security / Australia's interests of the alleged criminal conduct? (Harm may include physical harm to an individual, group or community, financial, reputational, loss of public confidence, damage to relationships etc) (If this report relates to the release of Commonwealth information, a harm statement from the agency head or delegate must be provided within this form or attached).[663]

658 AFP, *Submission 18*, 4.
659 AFP, *Submission 18*, 4.
660 Ms Krissy Barrett, Acting Deputy Commissioner, AFP, *Public hearing transcript*, 25 March 2024, 88.
661 AFP, *Submission 18*, 6–7.
662 Ms Krissy Barrett, Acting Deputy Commissioner, AFP, *Public hearing transcript*, 25 March 2024, 88–9.
663 AFP, 'Agency Report a Crime to the AFP form' (Form, 2023) 3. A copy of this form is published on the INSLM website as part of AFP, *Submission 18*.

10.46 This 'harm statement' may be iteratively developed through repeated consultation with the referring or affected agency but ultimately allows AFP to assess the seriousness of the alleged conduct.[664] AFP said, 'The reporting agency is best placed to understand the harm and the potential impact of a secrecy offence … and advise the AFP of this in an appropriate manner'.[665] AFP relies on the agency's initial assessment to inform other considerations that may impact assessment of harm, including:

- public interest considerations in protecting a free and open press
- whether there is suspected involvement of a foreign principal or their proxy
- whether the conduct (and hence the harm) is ongoing, recent or historical
- whether the classification of the materials has changed with time
- whether the person of interest (POI) occupies a position of significant trust or responsibility in the agency
- the experience or training of the POI in the handling of classified material
- the seriousness of the alleged offending in all the circumstances
- whether agencies are willing to commit to signed witness statements
- whether the POI has a lawful reason to access the material in the course of their duties, and
- whether the use of evidence in a prosecution may be affected by claims of parliamentary privilege.[666]

10.47 The apparent effect of the OPM and its regard to harm is that it is unlikely that a potential breach of a secrecy provision would be given high priority or even proceed through the investigation process if there was very little or no evidence of actual or likely harm.

10.48 AFP said, and I accept, that an agency's failure to provide a 'harm statement' or to agree to provide a witness to appear in court to describe the harm would also make it 'very difficult for [AFP] to satisfy the Director of Public Prosecutions prosecution policy'.[667]

664 AFP, *Submission 18*, 6; Mr Stephen Nutt, Acting Assistant Commissioner, AFP, *Public hearing transcript*, 25 March 2024, 89.
665 AFP, *Submission 18*, 6.
666 AFP, *Submission 18*, 6.
667 Mr Stephen Nutt, Acting Assistant Commissioner, AFP, *Public hearing transcript*, 25 March 2024, 90.

National Guideline on Sensitive Investigations

10.49 The Lawler Review also precipitated the AFP *National Guideline on Sensitive Investigations*.[668] The guideline entered into force in January 2020 and applies to any investigations that meet the definition of 'sensitive investigation'. A 'process of inquiry' will satisfy this definition where:

- it is, or possibly would be, of significant interest to the Australian community, and
- it involves, or is likely to impact on and/or be of significant interest to, a range of delineated circumstances, including Australia's international relationships or agreements, or a professional journalist or news media organisation, or
- the AFP Commissioner declares it to be a sensitive investigation.[669]

10.50 When a sensitive investigation is identified, it must be brought to the attention of the relevant Commander and then briefed to the responsible Assistant Commissioner. This framework intends to provide additional scrutiny of sensitive investigations by ensuring senior staff involvement, regular review and wider consultation where appropriate, as well as the application of enhanced risk management.

10.51 The guideline provides that a sensitive investigation may be escalated to the Sensitive Investigations Oversight Board for additional oversight and strategic consideration by senior executives in a range of circumstances. These notably include serious unauthorised disclosure investigations and where the investigation involves obtaining evidence from or about a professional journalist or news organisation.[670]

10.52 The guideline does not mean that an investigation for a secrecy offence involving a journalist or news media organisation will not proceed, and that should not be the result. But it does mean that investigations of this type do, as they should, get senior oversight, including to ensure that the 'importance of a free and open press in Australia's democratic society and … the broader public interest implications' are considered at every 'investigative action' point, consistent with the Attorney-General's direction.[671]

668 AFP, National Guideline on Sensitive Investigations (Guideline, August 2023).
669 AFP, National Guideline on Sensitive Investigations (Guideline, August 2023) 2.
670 AFP, National Guideline on Sensitive Investigations (Guideline, August 2023) 5-6.
671 Attorney-General (Cth), *Ministerial Direction (Australian Federal Police): Australian Federal Police Act 1979*, 20 October 2023.

Prosecution Policy of the Commonwealth and the 'public interest'

10.53 The Prosecution Policy of the Commonwealth is a significant and longstanding policy that underpins all of the decisions made by CDPP throughout the prosecution process. It applies to all Commonwealth prosecutions.[672] The policy outlines the relevant factors and considerations that are taken into account when Commonwealth prosecutors are exercising their discretion.

10.54 The policy requires CDPP to independently apply a 2-stage test before any prosecution is commenced:

- there must be sufficient evidence to justify the institution or continuation of a prosecution, and
- it must be evident, in light of the provable facts and the whole of the surrounding circumstances, that the public interest requires a prosecution to be pursued. [673]

10.55 In assessing the 'public interest', CDPP considers a range of factors, including the seriousness of the alleged offence, actual or potential harm occasioned to an individual and the availability of any alternatives to prosecution, such as effective disciplinary proceedings. The policy also expressly requires consideration of the seriousness, or relative triviality, of the alleged offence.[674]

10.56 The practical effect of the prosecution policy is that CDPP makes a robust and independent decision based on both the sufficiency of the evidence and public interest considerations before any prosecution, including a prosecution for a secrecy offence, is initiated. As noted earlier in this chapter, in matters where the Attorney-General's consent is required, CDPP forms their independent view on the public interest in a prosecution *before* a matter is submitted to the Attorney-General seeking consent.

10.57 I agree with AHRC's submission that, regardless of its robustness, appropriateness and efficacy, the policy does 'not replace the need for more tightly framed secrecy provisions in

672 Commonwealth Director of Public Prosecutions (CDPP), *Prosecution Policy of the Commonwealth: Guidelines For The Making of Decisions in the Prosecution Process* (Policy, 19 July 2021) ('Prosecution Policy of the Commonwealth').

673 CDPP advised that, where there are specific defences or exemptions for conduct performed in a journalist capacity, this will be taken into account by the prosecution in assessing whether there is a reasonable prospect of conviction. (i.e. before any consideration of public interest factors): Email from CDPP to INSLM, 8 May 2024.

674 See *Prosecution Policy of the Commonwealth* (n 672) 5-6 [2.8]–[2.14].

Part 5.6. of the Criminal Code'.[675] But that does not mean the prosecution policy does not play an important role.

Proposal for further guidance to CDPP

10.58 HRLC suggested that the Attorney-General should issue guidelines or a direction to CDPP setting out the matters to be considered when deciding whether to prosecute whistleblowers or journalists.[676] This would presumably be in addition to the current direction that the Director must not proceed with a prosecution of a journalist for certain offences without the Attorney-General's written consent.[677]

10.59 In their supplementary submission HRLC acknowledged that CDPP's prosecution policy already contains an extensive list of non-exhaustive public interest factors to be considered. Nevertheless, it suggested that 'these existing criteria in the Policy can be more relevant and explicitly targeted to decisions to prosecute whistleblowers and journalists, given the democratic implications'.[678] It points to the Ministerial Direction given to the AFP relating to journalists. As noted above, under that direction:

> [AFP must] take into account the importance of a free and open press in Australia's democratic society and to consider the broader public interest implications before considering investigative action involving a professional journalist or news media organisation.[679]

10.60 HRLC also set out a number of other factors specific to whistleblowers that could be taken into account.[680]

Does CDPP already consider the public interest in a free press?

10.61 As HRLC has noted, the list of public interest factors in the prosecution policy is non-exhaustive. The list does not expressly refer to the benefits of a free press or whether a particular disclosure had a public benefit. The closest item in the existing list of public interest factors is probably 'the necessity to maintain public confidence in the rule of law and the

675 AHRC, *Submission 17*, 21 [85].

676 HRLC, *Submission 14*, 10; HRLC, *Supplementary submission 23*, 1–2. Guidelines or directions can be issued by the Attorney-General under s 8 of the *Director of Public Prosecutions Act 1983* (Cth) or by CDPP, as provided for by s 11.

677 Attorney-General (Cth), *Ministerial Direction (Commonwealth Director of Public Prosecutions): Director of Public Prosecutions Act 1983*, 30 September 2019.

678 HRLC, *Supplementary submission 23*, 2.

679 Attorney-General (Cth), *Ministerial Direction (Australian Federal Police): Australian Federal Police Act 1979*, 20 October 2023.

680 HRLC, *Supplementary submission 23*, 1.

administration of justice through the institutions of democratic governance including the Parliament and the Courts'.[681]

10.62 CDPP suggested that there are also other factors in the list which may be relevant:

- mitigating or aggravating circumstances impacting on the appropriateness or otherwise of the prosecution
- the effect on community harmony and public confidence in the administration of justice
- the prevalence of the alleged offence and the need for deterrence, both personal and general
- whether the consequences of any resulting conviction would be unduly harsh and oppressive
- whether the alleged offence is of considerable public concern.[682]

10.63 CDPP advised this review that the importance of a free and open press in Australia's democratic society is a public interest that can be, and already is, considered under the current policy. CDPP provided the following actual example:

> The CDPP received a brief of evidence in relation to journalist [name omitted]. The brief of evidence was assessed in accordance with the Prosecution Policy of the Commonwealth and it was determined that there was a reasonable prospect of conviction in relation to some of the charges. However, having been satisfied that there was sufficient evidence to justify the initiation of a prosecution, the prosecutor then considered whether the public interest required a prosecution to be pursued. A range of factors were considered in assessing whether the public interest required a prosecution to be commenced in relation to [name omitted], including the role of public interest journalism. After careful consideration of a range of factors, it was determined that the public interest did not require a prosecution.

10.64 It is clearly open to CDPP to consider the public interest in maintaining a free and open press under the existing policy, and I accept that it has been a factor in actual cases.

Recommendation on prosecution policy

10.65 Prosecutions for secrecy offences involving journalists uniquely require consideration of the role of a free press, including in exposing corruption or other wrongdoing by government officials. While CDPP can already take this into account under the general concept of public

681 *Prosecution Policy of the Commonwealth* (n 672) 6 [2.10 (u)].

682 *Prosecution Policy of the Commonwealth* (n 672) 6–7 [2.10 (b), (g), (k), (l), (m)].

interest, there is merit in explicitly including it in the list of public interest factors to be considered.[683]

10.66 The only downside that I can see with this proposal is that it adds length to an already long policy document. Based on CDPP's evidence, adding an additional factor specific to journalists would not require a change to CDPP's current practice. In my view, the benefit of expressly recognising the role of public interest journalism in the prosecution policy outweighs the extra couple of lines it would add to the length of the document.

10.67 To be clear, I am not suggesting that the role of a free press be the overriding consideration – only that it be added to the existing non-exhaustive list of factors to be considered. Whether this is done by amending one of the existing factors or adding a new one is a matter of drafting. As always, CDPP's final decision on whether, in its view, a particular prosecution is in the public interest will depend on the specific facts of the case.

RECOMMENDATION 15: Consideration should be given to revising to 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.

10.68 The final wording of any amendment to the Prosecution Policy of the Commonwealth is ultimately a matter for the Director of Public Prosecutions. In making this recommendation it is not my intention that specific words be used; just that an amendment to give effect to the idea of recognising the role of genuine public interest journalism in our democracy as a public interest factor.

10.69 HRLC's proposal also extended to the prosecution of whistleblowers. As noted in **Chapter 1**, whistleblower protections are the subject of a current review by AGD. As such any proposals on whistleblowers need to be considered in the context of whatever recommendations that review makes. I make no finding on the matter here beyond suggesting that the public interest test in the Prosecution Policy of the Commonwealth is a matter AGD could consider in its whistleblower review.

683 That the AFP should have already considered the public interest in a free and open press does not detract from the need for CDPP to form its own independent view on how this matter affects the overall public interest in a prosecution. There are many factors which must be considered by both AFP and CDPP independently, including harm and the availability of defences.

Possible additional administrative measures

10.70 There are many ways to reduce the risk of sensitive government information being disclosed in a way that causes harm, including due to the threat of foreign interference and espionage. The need to take actions that do not involve prosecutions appears to be a point of potential consensus between government and non-government entities.

10.71 The Director-General of Security acknowledged this in his recent annual threat assessment, where he said, 'Yes, prosecutions are important … but there are other ways to efficiently and effectively reduce harm, particularly from espionage and foreign interference'.[684]

10.72 The Law Council emphasised that the solution to countering foreign interference is not necessarily to criminalise the innocuous conduct of civil society actors:

> At a time of heightened risk of foreign interference, the need to strengthen civil society information security may be a legitimate objective. However, ill-defined criminal offences are not an effective or necessary means of achieving that objective.[685]

Advice on safeguarding information

10.73 One of the concerns that intelligence agencies expressed was that, once sensitive information is out of their control and in the possession of media organisations, it is vulnerable to being acquired by foreign intelligence agencies, even if not 'published'.

10.74 On the storage and protection of information, Mr Paul Farrell, MEAA, said:

> I just make that point that, it's not like people are storing national security documents on public email servers or banding them around or things like that. There's a level of sophistication that I think is perhaps not always acknowledged or understood about the manner in which we would deal with some of those matters.[686]

10.75 ARTK addressed this point in its supplementary submission, saying there is a 'fundamental misunderstanding of journalistic practice and the sophistication with which confidential source derived material is handled. No evidence supports the suggestion that material provided by sources is unsafe or at risk of unlawful access by any hostile actor'.[687]

---

684 Mr Mike Burgess, 'Director-General's Annual Threat Assessment 2024' (Speech, Australian Security Intelligence Organisation, 28 February 2024).

685 Mr Philip Boulten SC, Law Council of Australia, *Public hearing transcript*, 25 March 2024, 162–3.

686 Mr Paul Farrell, MEAA, *Public hearing transcript,* 26 March 2024, 126.

687 ARTK, *Supplementary submission 21,* 10.

10.76 ARTK suggested that a more constructive approach be taken to supporting media organisations that deal with national security related information in their work:

> the intelligence services … [should] work with the media on a harm minimisation framework designed to ensure that journalists are otherwise aware of behaviour which may indicate that they are being cultivated by foreign intelligence agencies. Rather than threatening journalists for doing their jobs or suggesting they form a duped 'fifth column' for foreign interference, intelligence services need to find a constructive approach to working with the media that respects the media's right to publish in the public interest.[688]

10.77 In a similar vein Mr Pender from HRLC stated that:

> rather than criminalising dealing with conduct by third parties, it might be better to ensure that collectively we all are having sort of robust protocols to ensure that … our information is not intercepted.[689]

10.78 The proposal for a constructive approach could extend to espionage risk and information security advice and is something that could be considered as part of the broader government strategy for countering foreign interference.

DSMA system

10.79 In the context of possible disclosure or publication of information by non-officials, the United Kingdom has a longstanding system, Defence Security Media Advisor Notice System (DSMA Notice System). AJF said:

> [The DSMA Notice System is intended to provide] an opportunity for journalists and news agencies to consult with the security agencies through an independent committee, which then publishes non-binding notices (Standing Notices) to guide the media on the publication of defence and security information. The Standing Notices provide very specific and narrowly cast advice about information that should not be published in any circumstances.[690]

10.80 In 2020 the Parliamentary Joint Committee on Intelligence and Security (PJCIS) recommended that consideration be given to the formulation of a mechanism to allow for journalists and media organisations, in the act of public interest journalism, to consult with the originating agency of national security classified information without the threat of investigation or prosecution. In addition to creating this type of mechanism, PJCIS supported intelligence and law enforcement agencies creating media liaison units. AGD has said that work to develop media liaison units within intelligence agencies is ongoing.

10.81 Discussions with some media representatives during this review suggested that presently, at least for some, there is not a level of trust that would enable a DSMA Notice System to work well in Australia. This is particularly so if it was not seen as sufficiently independent from

688 ARTK, *Supplementary submission 21*, 10.
689 Mr Keiran Pender, *Public hearing transcript*, 25 March 2024, 26.
690 AJF, *Submission 11*, [4.18].

intelligence and police agencies. However, as already suggested by the PJCIS, development of a similar mechanism might be a practical approach to assist in the protection of sensitive information, at least in the medium to longer term. This could be complemented by risk and information security advice for media and civil society groups as part of the broader foreign interference and espionage resilience strategy.

Acronyms and abbreviations

ABC	Australian Broadcasting Corporation
ABF	Australian Border Force
ACC Act	*Australian Crime Commission Act 2002* (Cth)
ACIC	Australian Criminal Intelligence Commission
ADF	Australian Defence Force
ADJR Act	*Administrative Decisions (Judicial Review) Act 1977* (Cth)
AFP Act	*Australian Federal Police Act 1979* (Cth)
AFP	Australian Federal Police
AGD	Attorney-General's Department
AGO	Australian Geospatial-Intelligence Organisation
AHRC	Australian Human Rights Commission
AJF	Alliance for Journalists' Freedom
ALRC	Australian Law Reform Commission
AML/CTF Act	*Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth)
APS	Australian Public Service
ARTK	Australia's Right to Know (coalition of media organisations)
ASD	Australian Signals Directorate
ASIC	Australian Securities & Investment Commission
ASIO Act	*Australian Security Intelligence Organisation Act 1979* (Cth)
ASIO	Australian Security Intelligence Organisation
ASIS	Australian Secret Intelligence Service
ATO	Australian Taxation Office
AUKUS	The trilateral security partnership between Australia, the UK and the US
AUSTEO	Australian Eyes Only
AUSTRAC	Australian Transaction Reports and Analysis Centre
CDPP	Commonwealth Director of Public Prosecutions
CLA	Civil Liberties Australia

Criminal Code	*Criminal Code Act 1995* (Cth)
DFAT	Department of Foreign Affairs and Trade
DIG	Defence Intelligence Group
DIO	Defence Intelligence Organisation
EFI Act	*National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth)
EFI Bill	National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2018 (Cth)
FOI Act	*Freedom of Information Act 1982* (Cth)
Home Affairs	Department of Home Affairs
HRLC	Human Rights Law Centre
ICCPR	*International Covenant on Civil and Political Rights*
IGIS	Inspector-General of Intelligence and Security
INSLM Act	*Independent National Security Legislation Monitor Act 2010* (Cth)
INSLM	Independent National Security Legislation Monitor
INTERPOL	International Criminal Police Organization
IS Act	*Intelligence Services Act 2001* (Cth)
MEAA	Media, Entertainment and Arts Alliance
NACC	National Anti-Corruption Commission
NIC	National Intelligence Community
NSI Act	*National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth)
ONI Act	*Office of National Intelligence Act 2018* (Cth)
ONI	Office of National Intelligence
OPM	Operational Prioritisation Model
PID Act	*Public Interest Disclosure Act 2013* (Cth)
PII	Public Interest Immunity
PJCHR	Parliamentary Joint Committee on Human Rights
PJCIS	Parliamentary Joint Committee on Intelligence and Security
POC Act	*Proceeds of Crime Act 2002* (Cth)
PSPF	Protective Security Policy Framework
Public Service Act	*Public Service Act 1999* (Cth)

SBS	Special Broadcasting Service
SD Act	*Surveillance Devices Act 2004* (Cth)
SIO	Special Intelligence Operation
SIOB	Sensitive Investigations Oversight Board
SLAID Act	*Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (Cth)
SRC Act	*Safety, Rehabilitation and Compensation Act 1988* (Cth)
TIA Act	*Telecommunications (Interception and Access) Act 1979* (Cth)
TSPA	Top Secret Privileged Access
TSPV	Top Secret Positive Vetting
UNHRC	United Nations Human Rights Committee

List of submissions

Submissions in response to Issues Paper:

No	Organisation or individual	Date received	Reference
01	Civil Liberties Australia	10 February 2024	CLA, *Submission 1*
02	Department of Home Affairs	28 February 2024	Home Affairs, *Submission 2*
03	Australian Law Reform Commission	28 February 2024	ALRC, *Submission 3*
04	Australian Signals Directorate	29 February 2024	ASD, *Submission 4*
05	Defence Intelligence Group	29 February 2024	DIG, *Submission 5*
06	Australian Security Intelligence Organisation	29 February 2024	ASIO, *Submission 6*
07	Attorney-General's Department	1 March 2024	AGD, *Submission 7*
08	Office of National Intelligence	1 March 2024	ONI, *Submission 8*
09	Media, Entertainment and Arts Alliance	1 March 2024	MEAA, *Submission 9*
10	Australian Secret Intelligence Service	1 March 2024	ASIS, *Submission 10*
11	Alliance for Journalists' Freedom	1 March 2024	AJF, *Submission 11*
12	Australia's Right to Know	4 March 2024	ARTK, *Submission 12*
13	Joint Academic submission – Dr Dominique Dalla-Pozza, Associate Professor Rebecca Ananian-Welsh, Professor Peter Greste, Dr Kieran Hardy & Ms Sarah Kendall	4 March 2024	Joint Academic Submission, *Submission 13*
14	Human Rights Law Centre	5 March 2024	HRLC, *Submission 14*
15	Australian Transaction Reports and Analysis Centre	6 March 2024	AUSTRAC, *Submission 15*

No	Organisation or individual	Date received	Reference
16	Australian Criminal Intelligence Commission	8 March 2024	ACIC, *Submission 16*
17	Australian Human Rights Commission	8 March 2024	AHRC, *Submission 17*
18	Australian Federal Police	8 March 2024	AFP, *Submission 18*
19	Law Council of Australia	18 March 2024	Law Council of Australia, *Submission 19*
20	Commonwealth Director of Public Prosecutions	1 March 2024	CDPP, *Submission 20*
24	National Archives of Australia	8 March 2024	National Archives of Australia, *Submission 24*
32	Bill Calcutt PSM (unpublished)	25 March 2024	

Supplementary submissions and responses following public hearing

Submission no	Organisation or individual	Date received	Reference
21	Supplementary submission – Australia's Right to Know	9 April 2024	ARTK, *Supplementary submission 21*
22	Supplementary submission – Media, Entertainment and Arts Alliance	12 April 2024	MEAA, *Supplementary submission, 22*
23	Supplementary submission – Human Rights Law Centre	15 April 2024	HRLC, *Supplementary submission 23*
25	Supplementary response – Department of Home Affairs	16 April 2024	Home Affairs, *Supplementary response 24*
26	Supplementary submission – Law Council of Australia	23 April 2024	Law Council of Australia, *Supplementary submission 26*
27	Supplementary response – Australian Signals Directorate	16 April 2024	ASD, *Supplementary response 27*
28	Supplementary response – Australian Federal Police	29 April 2024	AFP, *Supplementary response 28*
29	Supplementary response – Defence Intelligence Organisation (unpublished)	16 April 2024	DIG, *Supplementary response 29*
30	Supplementary response – Office of National Intelligence (unpublished)	16 April 2024	ONI, *Supplementary response 30*
31	Supplementary response – Australian Secret Intelligence Service (unpublished)	16 April 2024	

Annex A

Part 5.6 of the Criminal Code Act 1995 (Cth)

This annexure contains Part 5.6 of the *Criminal Code Act 1995* ('*Criminal Code*') and related definitions from other Acts as in force during the conduct of this review.

Part 5.6—Secrecy of information

Division 121—Preliminary

121.1 Definitions

(1) In this Part:

cause harm to Australia's interests means to:

(a) interfere with or prejudice the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth; or

(b) interfere with or prejudice the performance of functions of the Australian Federal Police under:

(i) paragraph 8(1)(be) of the *Australian Federal Police Act 1979* (protective and custodial functions); or

(ii) the *Proceeds of Crime Act 2002*; or

(c) harm or prejudice Australia's international relations in relation to information that was communicated in confidence:

(i) by, or on behalf of, the government of a foreign country, an authority of the government of a foreign country or an international organisation; and

(ii) to the Government of the Commonwealth, to an authority of the Commonwealth, or to a person receiving the communication on behalf of the Commonwealth or an authority of the Commonwealth; or

(f) harm or prejudice the health or safety of the Australian public or a section of the Australian public; or

(g) harm or prejudice the security or defence of Australia.

Commonwealth officer means any of the following:

(a) an APS employee;

(b) an individual appointed or employed by the Commonwealth otherwise than under the *Public Service Act 1999*;

(c) a member of the Australian Defence Force;

(d) a member or special member of the Australian Federal Police;

(e) an officer or employee of a Commonwealth authority;

(f) an individual who is a contracted service provider for a Commonwealth contract;

(g) an individual who is an officer or employee of a contracted service provider for a Commonwealth contract and who provides services for the purposes (whether direct or indirect) of the Commonwealth contract;

but does not include an officer or employee of, or a person engaged by, the Australian Broadcasting Corporation or the Special Broadcasting Service Corporation.

deal has the same meaning as in Part 5.2.

Note: For the meaning of ***deal*** in that Part, see subsections 90.1(1) and (2).

domestic intelligence agency means:

(a) the Australian Secret Intelligence Service; or
(b) the Australian Security Intelligence Organisation; or
(c) the Australian Geospatial-Intelligence Organisation; or
(d) the Defence Intelligence Organisation; or
(e) the Australian Signals Directorate; or
(f) the Office of National Intelligence.

foreign military organisation means:

(a) the armed forces of the government of a foreign country; or
(b) the civilian component of:
  (i) the Department of State of a foreign country; or
  (ii) a government agency in a foreign country;
that is responsible for the defence of the country.

information has the meaning given by section 90.1.

inherently harmful information means information that is any of the following:

(a) security classified information;
(c) information that was obtained by, or made by or on behalf of, a domestic intelligence agency or a foreign intelligence agency in connection with the agency's functions;
(e) information relating to the operations, capabilities or technologies of, or methods or sources used by, a domestic or foreign law enforcement agency.

international relations has the meaning given by section 10 of the *National Security Information (Criminal and Civil Proceedings) Act 2004*.

proper place of custody has the meaning given by section 121.2.

Regulatory Powers Act means the *Regulatory Powers (Standard Provisions) Act 2014*.

security classification has the meaning given by section 90.5.

security classified information means information that has a security classification.

security or defence of Australia includes the operations, capabilities or technologies of, or methods or sources used by, domestic intelligence agencies or foreign intelligence agencies.

(2) To avoid doubt, ***communicate*** includes publish and make available.

(3) For the purposes of a reference, in an element of an offence in this Part, to security classified information or security classification, strict liability applies to the element that:

(a) a classification is applied in accordance with the policy framework developed by the Commonwealth for the purpose (or for purposes that include the purpose) of identifying the information mentioned in subparagraph 90.5(1)(a)(i) or (ii); or

(b) a classification or marking is prescribed by the regulations as mentioned in paragraph 90.5(1)(b).

Note: See the definitions of ***security classified information*** in subsection (1) and ***security classification*** in section 90.5.

121.2 Definition of *proper place of custody*

(1) ***Proper place of custody*** has the meaning prescribed by the regulations.

(2) Despite subsection 14(2) of the *Legislation Act 2003*, regulations made for the purposes of subsection (1) of this section may prescribe a matter by applying, adopting or incorporating any matter contained in an instrument or other writing as in force or existing from time to time, if the instrument or other writing is publicly available.

122.1 Communication and other dealings with inherently harmful information by current and former Commonwealth officers etc.

Communication of inherently harmful information

(1) A person commits an offence if:

(a) the person communicates information; and

(b) the information is inherently harmful information; and

(c) the information was made or obtained by that person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity.

Note 1: For exceptions to the offences in this section, see section 122.5.

Note 2: The fault elements for this offence are intention for paragraph (1)(a) and recklessness for paragraphs (1)(b) and (c) (see section 5.6).

Penalty: Imprisonment for 7 years.

Other dealings with inherently harmful information

(2) A person commits an offence if:

(a) the person deals with information (other than by communicating it); and

(b) the information is inherently harmful information; and

(c) the information was made or obtained by that person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity.

Note: The fault elements for this offence are intention for paragraph (2)(a) and recklessness for paragraphs (2)(b) and (c) (see section 5.6).

Penalty: Imprisonment for 3 years.

Information removed from, or held outside, proper place of custody

(3) A person commits an offence if:
  (a) the person:
    (i) removes information from a proper place of custody for the information; or
    (ii) holds information outside a proper place of custody for the information; and
  (b) the information is inherently harmful information; and
  (c) the information was made or obtained by that person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity.

Note: The fault elements for this offence are intention for paragraph (3)(a) and recklessness for paragraphs (3)(b) and (c) (see section 5.6).

Penalty: Imprisonment for 3 years.

Failure to comply with direction regarding information

(4) A person commits an offence if:
  (a) the person is given a direction; and
  (b) the direction is a lawful direction regarding the retention, use or disposal of information; and
  (c) the person fails to comply with the direction; and
  (ca) the failure to comply with the direction results in a risk to the security of the information; and
  (d) the information is inherently harmful information; and
  (e) the information was made or obtained by that person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity.

Note: The fault elements for this offence are intention for paragraph (4)(c) and recklessness for paragraphs (4)(a), (b), (ca), (d) and (e) (see section 5.6).

Penalty: Imprisonment for 3 years.

122.2 Conduct by current and former Commonwealth officers etc. causing harm to Australia's interests

Communication causing harm to Australia's interests

(1) A person commits an offence if:
  (a) the person communicates information; and
  (b) either:
    (i) the communication causes harm to Australia's interests; or

(ii) the communication will or is likely to cause harm to Australia's interests; and

(c) the information was made or obtained by that person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity.

Note 1: For the definition of ***cause harm to Australia's interests***, see section 121.1.

Note 2: For exceptions to the offences in this section, see section 122.5.

Penalty: Imprisonment for 7 years.

Other conduct causing harm to Australia's interests

(2) A person commits an offence if:

(a) the person deals with information (other than by communicating it); and

(b) either:

(i) the dealing causes harm to Australia's interests; or

(ii) the dealing will or is likely to cause harm to Australia's interests; and

(c) the information was made or obtained by that person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity.

Penalty: Imprisonment for 3 years.

Information removed from, or held outside, proper place of custody

(3) A person commits an offence if:

(a) the person:

(i) removes information from a proper place of custody for the information; or

(ii) holds information outside a proper place of custody for the information; and

(b) either:

(i) the removal or holding causes harm to Australia's interests; or

(ii) the removal or holding will or is likely to cause harm to Australia's interests; and

(c) the information was made or obtained by that person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity.

Penalty: Imprisonment for 3 years.

Failure to comply with direction regarding information

(4) A person commits an offence if:

(a) the person is given a direction; and

(b) the direction is a lawful direction regarding the retention, use or disposal of information; and

(c) the person fails to comply with the direction; and

(d) either:

(i) the failure to comply causes harm to Australia's interests; or

(ii) the failure to comply will or is likely to cause harm to Australia's interests; and

(e) the information was made or obtained by that person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity.

Penalty: Imprisonment for 3 years.

122.3 Aggravated offence

(1) A person commits an offence against this section if:

(a) the person commits an offence against section 122.1 or 122.2 (the ***underlying offence***); and

(b) any of the following circumstances exist in relation to the commission of the underlying offence:

(ii) if the commission of the underlying offence involves a record—the record is marked with a code word, "for Australian eyes only" or as prescribed by the regulations for the purposes of this subparagraph;

(iii) the commission of the underlying offence involves 5 or more records each of which has a security classification;

(iv) the commission of the underlying offence involves the person altering a record to remove or conceal its security classification;

(v) at the time the person committed the underlying offence, the person held an Australian Government security clearance allowing the person to access information that has a security classification of at least secret.

Penalty:

(a) if the penalty for the underlying offence is imprisonment for 7 years—imprisonment for 10 years; or

(b) if the penalty for the underlying offence is imprisonment for 3 years—imprisonment for 5 years.

(2) There is no fault element for the physical element in paragraph (1)(a) other than the fault elements (however described), if any, for the underlying offence.

(4) To avoid doubt:

(a) a person does not commit an underlying offence for the purposes of paragraph (1)(a) if the person has a defence to the underlying offence; and

(b) a person may be convicted of an offence against this section even if the person has not been convicted of the underlying offence.

122.4 Unauthorised disclosure of information by current and former Commonwealth officers etc.

(1) A person commits an offence if:

(a) the person communicates information; and

(b) the person made or obtained the information by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity; and

(c) the person is under a duty not to disclose the information; and

(d) the duty arises under a law of the Commonwealth.

Penalty: Imprisonment for 2 years.

(2) Absolute liability applies in relation to paragraph (1)(d).

Sunset provision

(3) This section does not apply in relation to any communication of information that occurs after the end of 29 December 2024.

122.4A Communicating and dealing with information by non-Commonwealth officers etc.

Communication of information

(1) A person commits an offence if:

(a) the person communicates information; and

(b) the information was not made or obtained by the person by reason of the person being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity; and

(c) the information was made or obtained by another person by reason of that other person being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity; and

(d) any one or more of the following applies:

(i) the information has a security classification of secret or top secret;

(ii) the communication of the information damages the security or defence of Australia;

(iii) the communication of the information interferes with or prejudices the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth;

(iv) the communication of the information harms or prejudices the health or safety of the Australian public or a section of the Australian public.

Note 1: For exceptions to the offences in this section, see section 122.5.

Note 2: The fault elements for this offence are intention for paragraph (1)(a) and recklessness for paragraphs (1)(b) to (d) (see section 5.6).

Penalty: Imprisonment for 5 years.

Other dealings with information

(2) A person commits an offence if:

(a) the person deals with information (other than by communicating it); and

(b) the information was not made or obtained by the person by reason of the person being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity; and

(c) the information was made or obtained by another person by reason of that other person being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity; and

(d) any one or more of the following applies:

(i) the information has a security classification of secret or top secret;

(ii) the dealing with the information damages the security or defence of Australia;

(iii) the dealing with the information interferes with or prejudices the prevention, detection, investigation, prosecution or punishment of a criminal offence against of a law of the Commonwealth;

(iv) the dealing with the information harms or prejudices the health or safety of the Australian public or a section of the Australian public.

Note: The fault elements for this offence are intention for paragraph (2)(a) and recklessness for paragraphs (2)(b) to (d) (see section 5.6).

Penalty: Imprisonment for 2 years.

Proof of identity not required

(3) In proceedings for an offence against this section, the prosecution is not required to prove the identity of the other person referred to in paragraph (1)(c) or (2)(c).

122.5 Defences

Powers, functions and duties in a person's capacity as a public official etc. or under arrangement

(1) It is a defence to a prosecution for an offence by a person against this Division that:

(a) the person was exercising a power, or performing a function or duty, in the person's capacity as a public official or a person who is otherwise engaged to perform work for a Commonwealth entity; or

(b) the person communicated, removed, held or otherwise dealt with the information in accordance with an arrangement or agreement to which the Commonwealth or a Commonwealth entity is party and which allows for the exchange of information.

Note: A defendant may bear an evidential burden in relation to the matters in this subsection (see subsection (12) of this section and subsection 13.3(3)).

Information that is already public

(2) It is a defence to a prosecution for an offence by a person against this Division that the relevant information has already been communicated or made available to the public with the authority of the Commonwealth.

Note: A defendant bears an evidential burden in relation to the matters in this subsection (see subsection 13.3(3)).

Information communicated etc. to integrity agency

(3) It is a defence to a prosecution for an offence by a person against this Division that the person communicated the relevant information, or removed, held or otherwise dealt with the relevant information for the purpose of communicating it:

(a) to any of the following:

(i) the Inspector-General of Intelligence and Security, or a person covered by subsection 32(1) of the *Inspector-General of Intelligence and Security Act 1986*;

(ii) the Commonwealth Ombudsman, or another officer within the meaning of subsection 35(1) of the *Ombudsman Act 1976*;

(iia) the Australian Information Commissioner, a member of the staff of the Office of the Australian Information Commissioner, or a consultant engaged under the *Australian Information Commissioner Act 2010*;

(iii) the National Anti-Corruption Commissioner or another staff member of the NACC (within the meaning of the *National Anti-Corruption Commission Act 2022*);

(iv) the Inspector of the National Anti-Corruption Commission or a person assisting the Inspector (within the meaning of the *National Anti-Corruption Commission Act 2022*); and

(b) for the purpose of the Inspector-General, the Ombudsman, the Australian Information Commissioner, the National Anti-Corruption Commissioner or the Inspector of the National Anti-Corruption Commission (as the case requires) exercising a power, or performing a function or duty.

Note: A person mentioned in paragraph (3)(a) does not bear an evidential burden in relation to the matters in this subsection (see subsection (12)).

Information communicated etc. in accordance with the Public Interest Disclosure Act 2013 or the Freedom of Information Act 1982

(4) It is a defence to a prosecution for an offence by a person against this Division that the person communicated the relevant information, or removed, held or otherwise dealt with the relevant information for the purpose of communicating it, in accordance with:

(a) the *Public Interest Disclosure Act 2013*; or

(b) the *Freedom of Information Act 1982*.

Note: A defendant may bear an evidential burden in relation to the matters in this subsection (see subsection (12) of this section and subsection 13.3(3)).

Information communicated etc. for the purpose of reporting offences and maladministration

(4A) It is a defence to a prosecution for an offence by a person against this Division that the person communicated, removed, held or otherwise dealt with the relevant information for the primary purpose of reporting, to an appropriate agency of the Commonwealth, a State or a Territory:

(a) a criminal offence, or alleged criminal offence, against a law of the Commonwealth; or

(b) maladministration relating to the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth; or

(c) maladministration relating to the performance of functions of the Australian Federal Police under:

(i) the *Australian Federal Police Act 1979*; or

(ii) the *Proceeds of Crime Act 2002*.

Note: A defendant may bear an evidential burden in relation to the matters in this subsection (see subsection (12) of this section and subsection 13.3(3)).

Information communicated etc. to a court or tribunal

(5) It is a defence to a prosecution for an offence by a person against this Division that the person communicated the relevant information, or removed, held or otherwise dealt with the relevant information for the purpose of communicating it, to a court or tribunal (whether or not as a result of a requirement).

Note: A defendant bears an evidential burden in relation to the matters in this subsection (see subsection 13.3(3)).

Information communicated etc. for the purposes of obtaining or providing legal advice

(5A) It is a defence to a prosecution for an offence by a person against this Division that the person communicated, removed, held or otherwise dealt with the relevant information for the primary purpose of obtaining or providing, in good faith, legal advice in relation to:

(a) an offence against this Part; or

(b) the application of any right, privilege, immunity or defence (whether or not in this Part) in relation to such an offence;

whether that advice was obtained or provided before or after the person engaged in the conduct constituting the offence.

Note: A defendant bears an evidential burden in relation to the matters in this subsection (see subsection 13.3(3)).

Information communicated etc. by persons engaged in business of reporting news etc.

(6) It is a defence to a prosecution for an offence by a person against this Division that the person communicated, removed, held or otherwise dealt with the relevant information in the person's capacity as a person engaged in the business of reporting news, presenting current affairs or expressing editorial or other content in news media, and:

(a) at that time, the person reasonably believed that engaging in that conduct was in the public interest (see subsection (7)); or

(b) the person:

(i) was, at that time, a member of the administrative staff of an entity that was engaged in the business of reporting news, presenting current affairs or expressing editorial or other content in news media; and

(ii) acted under the direction of a journalist, editor or lawyer who was also a member of the staff of the entity, and who reasonably believed that engaging in that conduct was in the public interest (see subsection (7)).

Note: A defendant bears an evidential burden in relation to the matters in this subsection (see subsection 13.3(3)).

(7) Without limiting paragraph (6)(a) or (b), a person may not reasonably believe that communicating, removing, holding or otherwise dealing with information is in the public interest if:

(a) engaging in that conduct would be an offence under section 92 of the *Australian Security Intelligence Organisation Act 1979* (publication of identity of ASIO employee or ASIO affiliate); or

(b) engaging in that conduct would be an offence under section 41 of the *Intelligence Services Act 2001* (publication of identity of staff); or

(c) engaging in that conduct would be an offence under section 22, 22A or 22B of the *Witness Protection Act 1994* (offences relating to Commonwealth, Territory, State participants or information about the national witness protection program); or

(d) that conduct was engaged in for the purpose of directly or indirectly assisting a foreign intelligence agency or a foreign military organisation.

Information that has been previously communicated

(8) It is a defence to a prosecution for an offence by a person against this Division if:

(a) the person did not make or obtain the relevant information by reason of any of the following:

(i) his or her being, or having been, a Commonwealth officer;

(ii) his or her being otherwise engaged to perform work for a Commonwealth entity;

(iii) an arrangement or agreement to which the Commonwealth or a Commonwealth entity is party and which allows for the exchange of information; and

(b) the information has already been communicated, or made available, to the public (the ***prior publication***); and

(c) the person was not involved in the prior publication (whether directly or indirectly); and

(d) at the time of the communication, removal, holding or dealing, the person believes that engaging in that conduct will not cause harm to Australia's interests or the security or defence of Australia; and

(e) having regard to the nature, extent and place of the prior publication, the person has reasonable grounds for that belief.

Note: A defendant bears an evidential burden in relation to the matters in this subsection (see subsection 13.3(3)).

Information relating to a person etc.

(9) It is a defence to a prosecution for an offence by a person against this Division if:

(a) the person did not make or obtain the relevant information by reason of any of the following:

(i) his or her being, or having been, a Commonwealth officer;

(ii) his or her being otherwise engaged to perform work for a Commonwealth entity;

(iii) an arrangement or agreement to which the Commonwealth or a Commonwealth entity is party and which allows for the exchange of information; and

(b) at the time of the communication, removal, holding or dealing, the person believes that the making or obtaining of the information by the person was required or authorised by law; and

(c) having regard to the circumstances of the making or obtaining of the information, the person has reasonable grounds for that belief; and

(d) any of the following apply:

(i) the person communicates the information to the person to whom the information relates;

(ii) the person is the person to whom the information relates;

(iii) the communication, removal, holding or dealing is in accordance with the express or implied consent of the person to whom the information relates.

Note: A defendant bears an evidential burden in relation to the matters in this subsection (see subsection 13.3(3)).

(10) To avoid doubt, a defence to an offence may constitute an authorisation for the purposes of paragraph (9)(b).

Removing, holding or otherwise dealing with information for the purposes of communicating information

(11) For the purposes of subsection (3), (4), (5) or (5A), it is not necessary to prove that information, that was removed, held or otherwise dealt with for the purposes of communicating it, was actually communicated.

Burden of proof for integrity agency officials

(12) Despite subsection 13.3(3), in a prosecution for an offence against this Division, a person mentioned in subparagraph (3)(a)(i), (ii), (iia) or (iii) does not bear an evidential burden in relation to the matter in:

(a) subsection (1), (4) or (4A); or

(b) either of the following:

(i) subparagraph (3)(a)(i), (ii), (iia) or (iii);

(ii) paragraph (3)(b), to the extent that that paragraph relates to the Inspector-General of Intelligence and Security, the Ombudsman, the Australian Information Commissioner, the National Anti-Corruption Commissioner or the Inspector of the National Anti-Corruption Commission.

Defences do not limit each other

(13) No defence in this section limits the operation of any other defence in this section.

Division 123—Miscellaneous

123.1 Injunctions

Enforceable provisions

(1) The provisions of Division 122 are enforceable under Part 7 of the Regulatory Powers Act.

Note: Part 7 of the Regulatory Powers Act creates a framework for using injunctions to enforce provisions.

Authorised person and relevant court

(2) For the purposes of Part 7 of the Regulatory Powers Act, as that Part applies to the provisions of Division 122 of this Act:

(a) the Minister is an authorised person; and

(b) each of the following is a relevant court:

(i) the Federal Court of Australia;

(ii) the Federal Circuit and Family Court of Australia (Division 2);

(iii) a court of a State or Territory that has jurisdiction in relation to matters arising under this Act.

Extension to external Territories

(3) Part 7 of the Regulatory Powers Act, as that Part applies to the provisions of Division 122 of this Act, extends to every external Territory.

123.2 Forfeiture of articles etc.

(1) A sketch, article, record or document which is made, obtained, recorded, retained, possessed or otherwise dealt with in contravention of this Part is forfeited to the Commonwealth.

(2) In subsection (1), ***sketch***, ***article*** and ***record*** have the same respective meanings as in Part 5.2.

123.3 Extended geographical jurisdiction—category D

Section 15.4 (extended geographical jurisdiction—category D) applies to an offence against this Part.

123.4 Effect of this Part on other rights, privileges, immunities or defences

Nothing in this Part limits or affects any other right, privilege, immunity or defence existing apart from this Part.

123.5 Requirements before proceedings can be initiated

(1) Proceedings for the commitment of a person for trial for an offence against this Part must not be instituted without:

(a) the written consent of the Attorney-General; and

(b) for proceedings that relate to security classified information—a certification by the Attorney-General that, at the time of the conduct that is alleged to constitute the offence, it was appropriate that the information had a security classification.

(2) However, the following steps may be taken (but no further steps in proceedings may be taken) without consent or certification having been obtained:

(a) a person may be arrested for the offence and a warrant for such an arrest may be issued and executed;

(b) a person may be charged with the offence;

(c) a person so charged may be remanded in custody or on bail.

(3) Nothing in subsection (2) prevents the discharge of the accused if proceedings are not continued within a reasonable time.

(4) In deciding whether to consent, the Attorney-General must consider whether the conduct might be authorised in a way mentioned in section 122.5.

Related definitions

This section provides the definitions of terms contained in Part 5.6 but defined elsewhere in the *Criminal Code* or other Acts.

Definitions from the Criminal Code Dictionary

Australian Government security clearance means a security clearance given by the Australian Government Security Vetting Agency or by another Commonwealth, State or Territory agency that is authorised or approved by the Commonwealth to issue security clearances.

Commonwealth authority means a body established by or under a law of the Commonwealth, but does not include:

(a) a body established by or under:

(ii) the *Australian Capital Territory (Self-Government) Act 1988*; or

(iii) the *Corporations Act 2001*; or

(iv) the *Norfolk Island Act 1979*; or

(v) the *Northern Territory (Self-Government) Act 1978*; or

(aa) a corporation registered under the *Corporations (Aboriginal and Torres Strait Islander) Act 2006*; or

(ab) an organisation registered, or an association recognised, under the *Fair Work (Registered Organisations) Act 2009*; or

(b) a body specified in the regulations.

Commonwealth contract *means a contract, to which a Commonwealth entity is a party, under which services are to be, or were to be, provided to a Commonwealth entity*

Commonwealth entity means:

(a) the Commonwealth; or

(b) a Commonwealth authority.

communication includes any communication:

(a) whether between persons and persons, things and things or persons and things; and

(b) whether the communication is:

(i) in the form of text; or

(ii) in the form of speech, music or other sounds; or

(iii) in the form of visual images (still or moving); or

(iv) in the form of signals; or

(v) in the form of data; or

(vi) in any other form; or

(vii) in any combination of forms.

contracted service provider, *for a Commonwealth contract, means:*

(a) a person who is a party to the Commonwealth contract and who is responsible for the provision of services to a Commonwealth entity under the Commonwealth contract; or
(b) a subcontractor for the Commonwealth contract.

foreign intelligence agency means an intelligence or security service (however described) of a foreign country.

harm means physical harm or harm to a person's mental health, whether temporary or permanent. However, it does not include being subjected to any force or impact that is within the limits of what is acceptable as incidental to social interaction or to life in the community.

make available, in relation to material, includes, but is not limited to, describing how to obtain access, or describing methods that are likely to facilitate access, to material (for example: by setting out the name of a website, an IP address, a URL, a password, or the name of a newsgroup).

serious harm means harm (including the cumulative effect of any harm):

(a) that endangers, or is likely to endanger, a person's life; or
(b) that is or is likely to be significant and longstanding.

Definitions from other sections of the Criminal Code

Part 2.2 – The elements of an offence

Section 5.2 Intention

(1) A person has intention with respect to conduct if he or she means to engage in that conduct.

(2) A person has intention with respect to a circumstance if he or she believes that it exists or will exist.

(3) A person has intention with respect to a result if he or she means to bring it about or is aware that it will occur in the ordinary course of events.

Section 5.4 Recklessness

(1) A person is reckless with respect to a circumstance if:
   (a) he or she is aware of a substantial risk that the circumstance exists or will exist; and
   (b) having regard to the circumstances known to him or her, it is unjustifiable to take the risk.

(2) A person is reckless with respect to a result if:
   (a) he or she is aware of a substantial risk that the result will occur; and
   (b) having regard to the circumstances known to him or her, it is unjustifiable to take the risk.

(3) The question whether taking a risk is unjustifiable is one of fact.

(4) If recklessness is a fault element for a physical element of an offence, proof of intention, knowledge or recklessness will satisfy that fault element.

Section 5.6 Offences that do not specify fault elements

(1) If the law creating the offence does not specify a fault element for a physical element that consists only of conduct, intention is the fault element for that physical element.

(2) If the law creating the offence does not specify a fault element for a physical element that consists of a circumstance or a result, recklessness is the fault element for that physical element.

Note: Under subsection 5.4(4), recklessness can be established by proving intention, knowledge or recklessness.

Section 6.1 Strict Liability

(1) If a law that creates an offence provides that the offence is an offence of strict liability:
   (a) there are no fault elements for any of the physical elements of the offence; and
   (b) the defence of mistake of fact under section 9.2 is available.

(2) If a law that creates an offence provides that strict liability applies to a particular physical element of the offence:
   (a) there are no fault elements for that physical element; and
   (b) the defence of mistake of fact under section 9.2 is available in relation to that physical element.

(3) The existence of strict liability does not make any other defence unavailable.

Part 5.2 – Espionage and related offences

Section 90.1 Definitions

(1) In this Part:

…

deal: a person ***deals*** with information or an article if the person does any of the following in relation to the information or article:

(a) receives or obtains it;
(b) collects it;
(c) possesses it;
(d) makes a record of it;
(e) copies it;
(f) alters it;
(g) conceals it;
(h) communicates it;
(i) publishes it;
(j) makes it available.

…

information means information of any kind, whether true or false and whether in a material form or not, and includes:

(a) an opinion; and
(b) a report of a conversation.

make available *information or an article includes:*

(a) place it somewhere it can be accessed by another person; and
(b) give it to an intermediary to give to the intended recipient; and
(c) describe how to obtain access to it, or describe methods that are likely to facilitate access to it (for example, set out the name of a website, an IP address, a URL, a password, or the name of a newsgroup).

…

prejudice: embarrassment alone is not sufficient to ***prejudice*** Australia's national security.

…

(2) In this Part, dealing with information or an article includes:

(a) dealing with all or part of the information or article; and

(b) dealing only with the substance, effect or description of the information or article.

(4) This Part applies to and in relation to a document or article regardless of who made it and what information it contains.

Section 90.5 Definition of security classification

(1) ***Security classification*** means:

(a) a classification of secret or top secret that is applied in accordance with the policy framework developed by the Commonwealth for the purpose (or for purposes that include the purpose) of identifying information:

(i) for a classification of secret—that, if disclosed in an unauthorised manner, could be expected to cause serious damage to the national interest, organisations or individuals; or

(ii) for a classification of top secret—that, if disclosed in an unauthorised manner, could be expected to cause exceptionally grave damage to the national interest; or

(b) any equivalent classification or marking prescribed by the regulations.

(1A) For the purposes of a reference, in an element of an offence in this Part, to security classification, strict liability applies to the element that:

(a) a classification is applied in accordance with the policy framework developed by the Commonwealth for the purpose (or for purposes that include the purpose) of identifying the information mentioned in subparagraph (1)(a)(i) or (ii); or

(b) a classification or marking is prescribed by the regulations as mentioned in paragraph (1)(b).

(2) Before the Governor-General makes regulations for the purposes of subsection (1), the Minister must be satisfied that the regulations are not inconsistent with the policy framework mentioned in paragraph (1)(a).

(3) Despite subsection 14(2) of the *Legislation Act 2003*, regulations made for the purposes of subsection (1) of this section may prescribe a matter by applying, adopting or incorporating any matter contained in an instrument or other writing as in force or existing from time to time, if the instrument or other writing is publicly available.

Extracts from other Acts

Australian Federal Police Act 1979 (Cth)

Section 8 Functions

(1) The functions of the Australian Federal Police are:

…

(be) to perform such protective and custodial functions as the Minister directs by notice in writing in the *Gazette*, being functions that relate to a person, matter or thing with respect to which the Parliament has legislative power; and

…

Section 8A Minister may direct which functions are protective service functions

The Minister may, by notice published in the *Gazette*, direct that certain protective and custodial functions of the Australian Federal Police are protective service functions.

National Security Information Act 2004 (Cth)

Section 10 Meaning of *international relations*

In this Act, ***international relations*** means political, military and economic relations with foreign governments and international organisations.

Acts Interpretation Act 1901 (Cth)

Section 2B Definitions

document means any record of information, and includes:

(a) anything on which there is writing; and
(b) anything on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them; and
(c) anything from which sounds, images or writings can be reproduced with or without the aid of anything else; and
(d) a map, plan, drawing or photograph.

…

record includes information stored or recorded by means of a computer.

Annex B

Previous reviews into secrecy offences

This annexure contains a very brief summary of relevant outcomes from the main parliamentary, government and independent reviews which looked at secrecy offences between 1991 and May 2024. Each of these reviews was considered in the development of this report.

Gibbs Committee Review of Commonwealth Criminal Law (1991)

Sir Harry Gibbs led a wide-ranging review of Commonwealth criminal law.[1] In relation to secrecy provisions, the review recommended that the application of the criminal law and sanctions in relation to unauthorised disclosures should be avoided where possible.[2] However, the review said that disclosure of information relating to intelligence and security services, defence or foreign relations, and information obtained in confidence from other governments or international organisations should be the subject of criminal sanctions.[3]

ALRC 2004 Keeping Secrets Report

In 2004 the Australian Law Reform Commission (ALRC) released the *Keeping Secrets: The Protection of Classified and Security Sensitive Information Report.*[4] This report was focused on safeguarding classified and security sensitive information during legal proceedings and investigations. In regard to secrecy provisions, the report said that criminal offences should only be imposed in relation to information that genuinely requires protection and where unauthorised disclosure is likely to harm the public interest. ALRC said that a clear distinction should be drawn between conduct that gives rise to administrative sanctions and conduct that gives rise to criminal sanctions.[5]

1 Sir Harry Gibbs, R.S Watson and A.C.C Menzies, *Review of Commonwealth Criminal Law* (Final Report, December 1991) ('*Gibbs Committee Review*').
2 *Gibbs Committee Review* (n 1) 315.
3 *Gibbs Committee Review* (n 1) 317.
4 Australian Law Reform Commission (ALRC), *Keeping Secrets: The Protection of Classified and Security Sensitive Information* (Report No 98, May 2004) ('*ALRC 2004 Keeping Secrets Report*').
5 *ALRC 2004 Keeping Secrets Report* (n 4) 18, recommendation 5-3.

ALRC 2009 Secrecy Laws Report

The 2009 ALRC report *Secrecy Laws and Open Government in Australia* (ALRC 2009 Secrecy Laws Report) recommended the repeal of the wide 'catch-all' secrecy provisions in ss 70 and 79 of the *Crimes Act 1914* (Cth) and the introduction of a new 'general secrecy offence' to protect 'essential public interests'.[6] A key recommendation was the adoption of a harm-based approach to ensure that criminal sanctions were 'reserved for behavior that harms, is reasonably likely to harm or intended to harm essential public interests'.[7] These were defined as:

- damage the security, defence or international relations of the Commonwealth;
- prejudice the prevention, detection, investigation, prosecution or punishment of criminal offences;
- endanger the life or physical safety of any person; or
- prejudice the protection of public safety.[8]

INSLM Report on Section 35P of the ASIO Act (2015)

The 2015 INSLM review titled *Report on the impact on journalists of section 35P of the ASIO Act* concluded that any restriction on the freedom of expression of journalists should be proportional to maintaining national security.[9] As a result, s 35P was amended such that the offence would only apply to members of the public (including journalists) where the disclosure would endanger the health or safety of a person or prejudice the conduct of a special intelligence operation. The requisite fault element is recklessess. However, the amendments also provide for an aggravated offence where the person knew or intended to endanger the health or safety of a person or prejudice the conduct of a special intelligence operation.[10]

Parliamentary Committee consideration of the EFI Bill (2018)

The National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 (EFI Bill) was first introduced to the parliament in December 2017 as part of a package of 3 separate Bills aimed at combatting the threat of foreign states and actors interfering in

6 ALRC, *Secrecy Laws and Open Government in Australia* (Report No 112, December 2009) ('*ALRC 2009 Secrecy Laws Report').*

7 *ALRC 2009 Secrecy Laws Report* (n 6) 23-4.

8 *ALRC 2009 Secrecy Laws Report* (n 6) 23-4.

9 Roger Gyles, INSLM (former), *Report on the Impact on Journalists of Section 35P of the ASIO Act* (Report, October 2015).

10 *Australian Secret Intelligence Organisation Act 1979* (Cth) s 35P.

Australia's political and electoral systems. It was reviewed by the Parliamentary Joint Committee on Intelligence and Security (PJCIS), Parliamentary Joint Committee on Human Rights (PJCHR) and the Senate Standing Committee for the Scrutiny of Bills. During the conduct of these reviews it became apparent that there was widespread concern about the breadth of the new secrecy offences and whether they unjustifiably limited freedom of expression in Australia. These concerns were voiced in particular by civil society groups (e.g. the Law Council of Australia and the Human Rights Law Centre) who had not been consulted on the Bill during its drafting.

Each committee produced a detailed report.[11] In March 2018, the Attorney-General provided proposed amendments to the Bill to the PJCIS before it reported, which addressed a number of concerns levelled at the new offences. In June 2018, the PJCIS tabled a report making 60 recommendations. The EFI Bill was amended in response to these recommendations.

2019 Comprehensive Review

Chapter 35 of the *Comprehensive Review of the Legal Framework of the National Intelligence Community* did not comment specifically on the then newly enacted Part 5.6 of the *Criminal Code* secrecy offences.[12] However, the review recommended retaining specific offences protecting the identity of Australian Secret Intelligence Service (ASIS) or Australian Secret Intelligence Organisation (ASIO) staff and agents and said these should not be extended to the Australian Signals Directorate (ASD) or Australian Defence Force Special Operations members.[13] It also recommended retaining the specific offences in the *Intelligence Services Act Act 2001* (Cth) (*IS Act*) though said these should be consolidated to reduce the chance of an individual charged with an offence being identified with a particular agency.[14] The review also considered, and rejected, the introduction of a general public interest disclosure exception for secrecy offences.[15]

---

11 Parliamentary Joint Committee on Intelligence and Security (PJCIS), Parliament of Australia, *Advisory Report on the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017* (Report, June 2018) 84-90 ('*PJCIS EFI Bill Report*'); Parliamentary Joint Committee on Human Rights (PJCHR), Parliament of Australia, Human Rights Scrutiny Report (Report No 2, 13 February 2018) 15-16; Senate Standing Committee for the Scrutiny of Bills, Parliament of Australia, *Scrutiny Digest 4 of 2018* (28 March 2018) 21.

12 Dennis Richardson, *Comprehensive Review of the Legal Framework of the National Intelligence Community* (Final Report, December 2019) vol 3, 99 [35.46] ('*2019 Comprehensive Review*').

13 *2019 Comprehensive Review* (n 12) vol 3, 111, recommendation 142. See also the *National Security Legislation Amendment (Comprehensive Review and Other Measures No.3) Act 2024* (Cth) sch 2.

14 See *2019 Comprehensive Review* (n 12) vol 3, 112-6 [35.108]–[35.131], recommendation 143.

15 See *2019 Comprehensive Review* (n 12) vol 3, 117-28 [35.132]–[35.179], recommendation 144.

PJCIS Press Freedom Report (2020)

In August 2020, the PJCIS completed its *Inquiry into the impact of the exercises of law enforcement and intelligence powers on the freedom of the press* (PJCIS Inquiry into Press Freedoms).[16] The report made recommendations about a range of laws and administrative mechanisms that affect press freedom. It suggested that defences for public interest journalism in other legislation be based on the defence in s 122.5(6) in Part 5.6 of the *Criminal Code*.[17]

Senate Environment and Communications References Committee Press Freedom Report (2021)

In May 2021, the Senate Environment and Communications References Committee reported on the adequacy of Commonwealth laws and frameworks covering the disclosure and reporting of sensitive and classified information. The Committee said it was:

> firmly of the view that the general secrecy offence provisions in the *Criminal Code* should include an express harm requirement, as recommended by the ALRC. Without such a requirement, the provisions would be susceptible to overuse, misuse or even abuse. In particular, the absence of an express harm requirement can lead to circumstances where a journalist is prosecuted for a very minor or trivial 'dealing' with classified information.[18]

INSLM NSI Act Review (2023)

The 2023 INSLM report into the *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth) included some consideration of the secrecy offences in that Act. In relation to those offences, the former Monitor recommended amendments to require that the disclosure be likely to prejudice national security.[19] This recommendation was intended to

---

16 PJCIS, *Inquiry into the Impact of the Exercise of Law Enforcement and Intelligence Powers on the Freedom of the Press* (Report, August 2020) ('*PJCIS Inquiry into Press Freedoms*').

17 *PJCIS Inquiry into Press Freedoms* (n 16) 98-9 [3.187]–[3.188], recommendation 7. During the review, the Attorney-General's Department (AGD), the Department of Home Affairs and the Law Council of Australia provided supplementary submissions in relation to certain issues that are relevant to this INSLM review, including the inclusion of an express harm requirement in div 122 of the *Criminal Code*; ambiguity in div 122; factors that may be considered for the purpose of determining whether the dealing with or holding of information may be in the public interest; and the onus to establish that a disclosure is not in the public interest.

18 Senate Environment and Communications References Committee, Parliament of Australia, *Freedom of the Press* (Report, May 2021) 35.

19 Grant Donaldson, INSLM (former), *Review into the operation and effectiveness of the National Security Information (Criminal and Civil Proceedings) Act 2004* (Report, 30 October 2023) ('*INSLM NSI Act Review*').

limit the breadth of the conduct captured, particularly in the context of disclosures to legal representatives where 'in many circumstances, the disclosure would not likely prejudice national security'.[20]

AGD Review of Secrecy Provisions (2023)

The 2018 PJCIS inquiry into the EFI Bill recommended a government review of the 'array of specific secrecy offences' outside the new Part 5.6 offences, and that the review take account of the principles from the ALRC 2009 Secrecy Laws Report.[21] The PJCIS Inquiry into Press Freedoms reiterated this recommendation. AGD recently undertook a review of this type – the AGD *Review of Secrecy Provisions*.[22] AGD recommended 12 principles to guide further work to reduce the number of secrecy offences and support a consistent approach to framing secrecy provisions. These principles include limiting offences to circumstances where there is an 'essential public interest', including an express harm element except in narrowly defined categories where harm is implicit, and that offences should clearly identify the conduct regulated.[23] The 12 principles set out by AGD as set out in Chapter 1 of its report appear broadly consistent with earlier reviews.

The AGD Review of Secrecy Provisions also made other recommendations including that the general secrecy offence in s 122.4 of the *Criminal Code* be replaced with a new general offence for Commonwealth officials and others who perform services for the Commonwealth to criminalise disclosures which would be 'prejudicial to the effective working of government' or 'where the information was communicated to them in confidence'.[24]

PJCIS review of the National Security Legislation Amendment (Comprehensive Review and Other Measures No. 3) Bill 2023 (2024)

In March 2024 the PJCIS released its report on the National Security Legislation Amendment (Comprehensive Review and Other Measures No. 3) Bill 2023.[25] Amongst other things, the Bill amends the secrecy offences in the *IS Act* by consolidating the offences that apply to the

---

20 *INSLM NSI Act Review* (n 19) [729].

21 *PJCIS EFI Bill Report* (n 11) [4.188]–[4.189], recommendation 24.

22 AGD, *Review of Secrecy Provisions* (Final Report, 21 November 2023) ('*AGD Review of Secrecy Provisions*').

23 *AGD Review of Secrecy Provisions* (n 22) recommendation 1.

24 *AGD Review of Secrecy Provisions* (n 22) recommendation 3.

25 National Security Legislation Amendment (Comprehensive Review and Other Measures No.3) Bill 2023 (Cth); PJCIS, *Advisory Report on the National Security Legislation Amendment (Comprehensive Review and Other Measures No.3) Bill 2023* (Report, March 2024) ('*PJCIS NSLAB3 Report*').

three agencies governed by that Act – ASIS, ASD, the Australian Geospatial-Intelligence Organisation – as well as the Defence Intelligence Organisation (DIO).[26]

These amendments raise some of the same issues that were considered in this INSLM review including: when a 'no harm' offence is appropriate; if such an offence is appropriate for intelligence officials (and contractors etc.); should it apply to non-intelligence functions or only intelligence related functions and capabilities; should the secrecy offences for at least the 6 main intelligence agencies be in the *Criminal Code* rather than replicated in the *IS Act*, *ASIO Act* and *Office of National Intelligence Act 2018* (Cth); and whether it is consistent with the rule of law to create offences that are dependent on the functions of DIO when DIO does not have any statutory functions and its functions can be changed by the executive at any time. For those reasons the PJCIS ultimately recommended that the government consider aligning its proposed amendments to secrecy offences contained in the *IS Act* and *ASIO Act* with relevant recommendations from *this review* pending the timing of its completion and passage of the legislation.[27] The Bill passed on 15 May 2024 without amendment to these provisions.

26 See National Security Legislation Amendment (Comprehensive Review and Other Measures No. 3) Bill 2023 (Cth) sch 2 pt 2 div 1 items 7-30; Explanatory Memorandum, National Security Legislation Amendment (Comprehensive Review and Other Measures No. 3) Bill 2023 (Cth) [144]–[178].

27 *PJCIS NSLAB3 Report* (n 25) recommendation 4.

Annex C

The INSLM Review process

The *Independent National Security Legislation Monitor Act 2010* (Cth) (*INSLM Act*) provides considerable scope for each Monitor to determine the process for each review conducted under that Act. This review began with introductory meetings with a range of government and non-government stakeholders. These preliminary discussions together with independent research and analysis led to the production of a detailed Issues Paper being released in January 2024. Throughout the course of the review I had many meetings with stakeholders. I also convened three roundtable meetings in February 2024 to provide a forum for the sharing of ideas and to test my preliminary views. Public hearings were held in March 2024. These provided an opportunity for stakeholders to respond to my preliminary views and make submission on issues of importance to them. I invited supplementary submissions following the hearing and also had a number of follow-up meetings. Agencies were consulted about text in the report that draws on information that they identified as classified or sensitive to ensure that the report does not include information of the type described in s 29(3) of the *INSLM Act*. In accordance with s 29B of the *INSLM Act* this report was provided to the Attorney-General.

I am very grateful to the many agencies, organisations and individuals who engaged with this review. Many provided detailed and considered submissions which greatly assisted with this review. I particularly acknowledge that many who provided input on behalf of civil society groups did so as volunteers contributing in their own time.

I was also greatly assisted by the staff of the INSLM office and by Kim Pham and Anthony Hall who provided advice as counsel assisting.

Issues Paper

On 18 January 2024 I wrote to a broad range of stakeholders to provide them with a copy of the Issues Paper for this review. The Issues Paper was also made available on the INSLM website. The 80-page issues paper provided background and analysis on the offences in Part 5.6 of the *Criminal Code* to support engagement with the review. The Issues Paper was accompanied by an annex containing comparable secrecy provisions from Five Eyes countries. The Issues Paper identified and discussed 35 potential issues arising out of Part 5.6 of the *Criminal Code*.

Roundtables

In early 2024 I convened three roundtables with key experts and stakeholders to identify and discuss potential issues with Part 5.6 as well as to test my preliminary ideas:

- Academic Roundtable – 1 February 2024 (Brisbane)
  - Professor Peter Greste, Macquarie University

- Associate Professor Rebecca Ananian-Welsh, University of Queensland
- Dr Keiran Hardy, Griffith University
- Dr Dominique Dalla-Pozza, The Australian National University
- Ms Sarah Kendall, University of Queensland

- Civil society group Roundtable – 2 February 2024 (Canberra)
  - Australia's Right to Know
  - Civil Liberties Australia
  - Human Rights Law Centre
  - Law Council of Australia
  - Media Entertainment & Arts Alliance
  - New South Wales Council for Civil Liberties
- National Intelligence Community Roundtable – 8 February 2024 (Canberra) which included all 10 National Intelligence Community agencies as well as the Attorney-General's Department and the Department of Home Affairs.

Summaries of the academic roundtable and civil society roundtable were published on the INSLM website.

Consultations and private meetings

I spoke with many individuals and organisations about the secrecy offences between December 2023 and May 2024. Consultations were held in-person in Brisbane, Sydney, Canberra and Melbourne, via phone and online. These included meetings with many of the National Intelligence Community agencies, Attorney-General's Department and Department of Home Affairs. I also had a number of meetings with the Commonwealth Department of Prosecutions. In addition, I met separately with each of the civil society groups who attended the 2 February roundtables as well as the Victorian Council for Civil Liberties and Queensland Council for Civil Liberties.

Notices to produce information under s 24 of the *INSLM Act* were issued at the request of some agencies in respect of some information (including about current investigations) to ensure that they could provide all requested information without risking a breach of secrecy or confidentiality obligations.

Submissions

I received 22 general submissions in response to the Issues Paper. I also received correspondence from the Inspector-General of Intelligence and Security in response to specific questions addressed to it. Following the public hearing I received 4 supplementary submissions as well as responses to questions on notice from 6 agencies. Almost all

submissions, supplementary submissions and questions on notice responses were made publicly available on the INSLM website. A small amount of material was provided in classified annexes or otherwise identified as not suitable for publication by the agencies providing it.

Public hearing

A public hearing was held on 25 and 26 March 2024 in Canberra. A live stream of the hearing was available and a transcript of the hearing is published on the INSLM website.

Representatives appeared from the following government agencies:

- Attorney-General's Department
  - Ms Sarah Chidgey, Deputy Secretary, National Security and Criminal Justice Group
- Australian Federal Police
  - Ms Krissy Barrett, Acting Deputy Commissioner
  - Mr Stephen Nutt, Acting Assistant Commissioner
- Australian Human Rights Commission
  - Ms Lorraine Finlay, Human Rights Commissioner
  - Ms Jane Fraser, Senior Lawyer
- Australian Secret Intelligence Organisation
  - Mr Mike Burgess, Director-General of Security
- Australian Signals Directorate
  - Mr Stephen McGlynn, Acting Chief Operating Officer
- Defence Intelligence Group
  - Lieutenant General Gavan Reynolds AO, Chief of Defence Intelligence
  - Mr Cameron Heath, Assistant Secretary, Intelligence Policy and Priorities
  - Air Commodore Patrick Keane AM CSC, Director-General Military Legal Service
- Department of Home Affairs
  - Mr Nathan Smyth, Deputy Secretary, National Security and Resilience
  - Mr James Robinson, Acting First Assistant Secretary, National Security
- Office of National Intelligence
  - Ms Nina Davidson, Deputy Director-General
  - Ms Susan Littlehales, Assistant Director-General, Executive

- Ms Jeustelle Staver, General Counsel

Non-government witnesses were:

- Alliance for Journalists' Freedom
  - Mr Peter Greste, Executive Director
  - Ms Phyllida Behm, Marque Lawyers
- Associate Professor Rebecca Ananian-Welsh, University of Queensland
- Australia's Right to Know
  - Ms Georgia-Kate Schubert, Policy and government affairs, News Corps Australia
  - Mr Robert Todd, Partner, Ashurst
- Dr Dominique Dalla-Pozza, Australian National University
- Dr Keiran Hardy, Griffith University
- Human Rights Law Centre
  - Mr Kieran Pender, Senior Lawyer
  - Ms Olivia Roney, Lawyer
- Law Council of Australia
  - Dr David Neal SC, National Criminal Law Committee
  - Mr Philip Boulten SC, National Criminal Law Committee
  - Mr Shounok Chatterjee, Policy Lawyer
- Media, Entertainment and Arts Alliance
  - Ms Lilia Anderson, Policy and strategic research lead
  - Mr Paul Farrell, Member

Annex D

Security classification training and internal guidance

As noted in **Chapter 4** and in **Annexure E** the Inspector-General of Intelligence and Security (IGIS) *Preliminary Inquiry into the application of national security classifications in ASIO, ASIS, ONI, ASD, AGO and DIO* found that:

- 30% of staff considered their training on making classification decisions to be inadequate.
- 20% said they were not aware of internal guidance or that it did not adequately equip them to make classification decisions.[1]

Despite this finding a number of agencies advised me that their staff are all well trained in how to make security classification decisions. I asked questions about this training at the public hearing however, most agencies were unable to provide much detail at that time (beyond saying they had mandatory annual security awareness training). I therefore sent out a number of questions on notice. This annex summarises those responses.

This does not represent a comprehensive review of Australian government agency training on security classification decision-making. Questions on notice were only put to six national intelligence community agencies. This sample was intended to provide an indication of what training was provided and what percentage of staff have undertaken it. As the focus of this part of the review is on the suitability of 'security classifications' as part of a *criminal offence*, this was the lens through which training and its uptake was analysed. I make no finding on whether the training is adequate for *administrative* purposes.

Some agencies provided information at an unclassified level while other agencies provided very similar information but marked it as classified. In the available time I chose not to prioritise pursuing this and have instead provided only a high-level summary as this is all that is required for the purpose of this review.

1 Inspector-General of Intelligence and Security (IGIS), *Preliminary Inquiry into the Application of National Security Classifications in ASIO, ASIS, ONI, ASD, AGO and DIO: Preliminary Inquiry Report* (Preliminary Report, 25 February 2021).

Questions about training

Agencies were asked:

1. Does [AGENCY] have mandatory training on how to correctly classify information in accordance with the Protective Security Policy Framework: Policy 8? How often does this training occur and what percentage of staff have completed it within the last training cycle?
2. Please provide (at a classified level, if necessary) a copy of your classification training materials including any slides, text and questions staff are required to answer. If your classification training sits within a wider training package, we only require the parts of the training that go to the classification of information.
3. Do [AGENCY] systems include automated or default classifications (e.g. 'reply to' emails)? If so, please describe how this operates.

Who can make classification decisions?

Anyone with the security clearance to access the information can classify information as secret or top secret. This is many thousands of individuals.[2]

General security awareness training

Annual security awareness training for all personnel is recommended by the Protective Security Policy Framework (PSPF), Policy 2: Management structures and responsibilities (PSPF Policy 2).[3] In accordance with that policy it is recommended that security awareness training cover a broad range of general security-related topics such as: an overview of protective security requirements; personal safety; individual and line-manager responsibilities; confidentiality, integrity and availability requirements for information and assets (including intellectual property); entity specific security risks; the 'need-to-know' principle; overseas travel safety; unusual and suspicious behaviour; asset protection; and, reporting requirements (security incidents, contact reporting, reporting concerns about other personnel and the Public Interest Disclosure scheme). Training on how to make security classification decisions is not specifically mentioned in the policy on annual awareness training, but could no doubt be included if an entity wished to add it.[4]

Every NIC agency conducts some form of basic security training on induction and in the form of an annual security awareness course. Annual training appears to be mostly delivered as an on-line training module. Several agencies provided this review with copies of their training

2 Mr Nathan Smyth, Department of Home Affairs, *Pubic Hearing Transcript*, 25 March 2024, 76;

3 Department of Home Affairs, Protective Security Policy Framework, Policy 2: Management and responsibilities (Policy No 2, August 2023) 16-17 [92]-[96] ('*PSPF Policy 2*').

4 *PSPF Policy 2* (n 3) 16-17 [92]-[95].

materials. That material appears consistent with the requirements of PSPF Policy 2, that is, it briefly covers the broad range of topics mentioned above.

None of the annual security awareness training reviewed provided any detailed guidance on making classification decisions.

- Defence Intelligence Group (DIG) (covering the Australian Geospatial-Intelligence Organisation (AGO) and the Defence Intelligence Organisation (DIO)) reported annual awareness training had been completed by around 90% of staff as of April (this figure is likely to be well over 90% by the end of the performance cycle on 30 June).[5]
- Similarly the Australian Federal Police (AFP) reported around 90% (with the figure likely to be higher by the end of the financial year).[6]
- For the Office of National Intelligence (ONI), the figure was closer to 50% so far in this financial year (2023-24). This did not include staff who had not yet worked at the agency for more than 12 months or who had completed their last annual module less than 12 months ago.[7]
- ASD provided a figure for how many staff had completed 'induction' training in the past 12 months but did not provide a response to the question about how many staff had completed annual security awareness training. [8]
- The Department of Home Affairs said that all staff were expected to undertake training. However, they did not provide any statistics on how many Home Affairs staff have undertaken annual security awareness training in the past 12 months. [9]

As noted above, the purpose of annual security awareness training is not to provide detailed guidance on classification. Most of the annual training is about the importance of ensuring that classified documents are properly stored and only shown to people with an appropriate clearance and a 'need to know'. Of the training materials reviewed the most detailed information provided on classification was a slide with a copy of the basic PSPF classification table (a copy of that table is reproduced in **Chapter 4** of this report).

Classification-specific training

The Department of Defence has created a specific training module called Assessing and Protecting Official Information (APOI). The course is not mandatory but it is recommended

5 Defence Intelligence Group (DIG), *Supplementary response 29.*
6 Australian Federal Police (AFP), *Supplementary response 28*, QON 2.
7 Office of National Intelligence (ONI), *Supplementary response 30*, 1.
8 Australian Signals Directorate (ASD), *Supplementary response 27,* 1.
9 Home Affairs, *Supplementary response 24,* 3.

that all Defence personnel undertake this web-based course every two years. The course material largely replicates the PSPF, Policy 8: Classification system (PSPF Policy 8) but includes some Department of Defence-specific examples. Across the three Defence intelligence agencies around 40% of staff have completed the on-line APOI module in the past two years.[10]

Home Affairs said that it 'provides ad-hoc protective security training (including on information classification handling) as and when the need arises'. However, it said that 'the Department does not hold statistical data on the number of staff who have been provided with this training over the last 12 months' and did not provide any training materials.[11]

AFP has 'information management training'. This training is primarily about general record keeping requirements and does not contain specific guidance on how to make classification decisions, although it is pleasing to see that training on record keeping has been completed by 94% of AFP appointees and contractors in that agency in the past 24 months.[12]

Internal Guidance

Most agencies have internal security guidance documents available for staff to refer to. Some documentation largely replicates PSPF Policy 8 with little additional information. Some are more detailed. For example, DIO has a fairly detailed guide to assist analysts in classifying documents. Examples in internal guidance materials provided by some other agencies were so broad that officials relying on those examples could easily make classification decisions that may not align with the requirements in s 90.5(1)(a). Internal materials also describe how to store classified information and where and in what colour classification markings are to be made. In terms of the risk of over-classification and under-classification, the consistent message in agency guidance materials is:

- Under-classifying 'constitutes a security breach' and 'risks compromise of sources, and jeopardises Australia's access to the sources and relationships that make privileged information available to us'.
- Over classification is a problem because 'high classification documents cost far more to manage' and 'they limit access to key information that many staff need'.

None of the guidance materials explained the interaction between the PSPF and the *Criminal Code* and the fact that classification decisions made by officials were relevant to the boundaries of the offences in Part 5.6.

---

10 DIG said that it was not satisfied with this level of currency and intend to make the course mandatory for all staff in the Defence Intelligence Organisation and Australian Geospatial-Intelligence Organisation: DIG, *Supplementary response 29;* ASD, *Supplementary response 27,* 1.

11 Home Affairs, *Supplementary response 24,* 3.

12 AFP, *Supplementary response 28,* QON 2.

Automated or default classifications

Where an email is received which already bears a classification, the same classification will automatically be applied to subsequent responses or forwards of that email. Three agencies said that users can change the default classification, but only to a *higher* classification. One said 'users are to confirm' the classification applied by the system. One said users can 'manually change' the classification.

In addition to email, one agency noted that some of their 'operational systems may assign information pre-determined security classifications, based on the sensitivity and classification of the specific operation or capability'.[13]

Related matters

In addition to the questions about training, I looked at the provided training material and internal guidance to see what it said about review of classification decisions and record keeping for classification decisions.

Review of classification decisions

At the hearing I asked a number of agencies whether they had a formal process for reviewing or auditing the classification decisions made by staff to understand whether over-classification or under-classification of information was occurring.

The PSPF *recommends* that agencies regularly review classified information for continuing sensitivity.[14]

No agency claimed or submitted evidence that they had a process for regular review. Two noted that if an *Archives Act 1983* (Cth) access request is made for historical records then the classification of that material is reviewed as part of that process.[15] One noted that it expects staff to consider if a security classification remains appropriate anytime a document is updated or amended.[16] ONI emphasised that only the originator could review a

13 ASD, *Supplementary response 27*, 2.

14 Department of Home Affairs, Protective Security Policy Framework, Policy 8: Classifications system (Policy No 8, October 2022) 10 [38] ('*PSPF Policy 8*'); Home Affairs, *Supplementary response 24,* 2.

15 Mr Mike Burgess, Director-General of Security, ASIO, *Public Hearing Transcript*, 25 March 2024, 13; Ms Susan Littlehales, ONI, *Public Hearing transcript*, 26 March 2024, 141.

16 AFP, *Supplementary response 28,* QON 3.

classification.[17] This is consistent with the PSPF Policy 8 which states that 'an entity must not remove or change information's classification without the originator's approval'.[18]

The originator is described in PSPF 8 as

> the entity that initially generated the information, or first received the unmarked information (ie an Australian Government or third-party approved security classification has not been applied) from outside the Australian Government, and assessed the value, importance or sensitivity … and assigned the corresponding protective marking or classification.[19]

The PSPF adds that

> The originator is usually the person that created or first assessed the information. However, to ensure continuity, the entity may set the originator as the person, role, delegation or section within the entity that is best placed to be responsible for controlling the information.

Record keeping

The PSPF does not require agencies to keep records of which individual made a classification decision or why. None of the internal guidance material or training on classification decision making require staff to keep records of the reasons for classification decisions. It may not be necessary to keep such records for administrative purposes (though presumably it would make review and audit easier), however, if a classification decision is challenged in a criminal proceeding a lack of records may be problematic for the prosecution.

In some cases (for example, original emails) it will be possible to ascertain who made a classification decision, though not necessarily why.

17 Ms Jeustelle Staver, ONI, *Public Hearing transcript*, 26 March 2024, 141; ONI, *Submission 8*, 3;
18 *PSPF Policy 8* (n 14) 3.
19 *PSPF Policy 8* (n 14) 5 [20].

Annex E

IGIS Preliminary Inquiry into security classifications

A number of submissions have referred to the Inspector-General of Intelligence and Security (IGIS) *Preliminary Inquiry into the application of national security classifications in ASIO, ASIS, ONI, ASD, AGO and DIO* (IGIS Security Classifications Preliminary Inquiry)[1]. For example, in its written submission the Office of National Intelligence said:

> *The IGIS found there was no evidence of systemic misunderstanding of the scope or application of classifications in the PSPF, which may have been expected if the PSPF was ambiguous or if thresholds for classifications (regardless of references to s90.5 of the Criminal Code) were too imprecise to allow consistent and defensible classification decisions.*[2]

The IGIS Security Classifications Preliminary Inquiry did not address whether it is appropriate to use the Protective Security Policy Framework (PSPF) and decisions made under it as part of the structure of a serious criminal offence. However, as several agencies sought to rely on the IGIS Security Classifications Preliminary Inquiry for this purpose it is important to understand the purpose of an IGIS preliminary inquiry and the actual findings of this particular preliminary inquiry.

What is an IGIS preliminary inquiry for?

The role of the IGIS is to assist Ministers to ensure that certain agencies act legally and with propriety, comply with ministerial guidelines and directives, and respect human rights.[3]

The *Inspector-General of Intelligence and Security Act 1986* (Cth) (*IGIS Act*) allows the Inspector-General to undertake a preliminary inquiry in order to determine whether a matter is within jurisdiction or to determine whether the Inspector-General should inquire into an action of an intelligence agency that is within jurisdiction.[4] If the Inspector-General then

1 Inspector-General of Intelligence and Security, *Preliminary Inquiry into the Application of National Security Classifications in ASIO, ASIS, ONI, ASD, AGO and DIO: Preliminary Inquiry Report* (Preliminary Report, 25 February 2021).

2 Office of National Intelligence (ONI), Submission 8, 9.

3 *Inspector-General of Intelligence and Security Act 1986* (Cth) s 4 ('*IGIS Act*').

4 *IGIS Act* (n 4) s 14.

decides to conduct a full inquiry this enlivens access to significant statutory powers as well as detailed notification and reporting requirements.[5]

The IGIS office is small relative to the size of the agencies it has oversight over. Preliminary inquiries can assist the Inspector-General to decide if there is a matter of sufficient concern as to legality, propriety, human rights or compliance with Ministerial directions that the diversion of resources from other tasks to conduct a full Inquiry is warranted.

The preliminary inquiry into security classifications was commenced in response to a recommendation by the Parliamentary Joint Committee on Intelligence and Security that the IGIS undertake such an action.[6]

What did the Preliminary inquiry find?

The IGIS Security Classifications Preliminary Inquiry involved three main activities: a review of intelligence agencies' policies and procedures in relation to security classification decisions, a survey of intelligence employees' views on issues relating to security classifications, and a review of a sample of documents to assess the appropriateness of their security classifications.[7]

In this final activity, the classified material review, IGIS staff reviewed over 100 security classification decisions from across the six agencies within IGIS jurisdiction at the time. These document were described as 'significant documents...including ministerial submissions, intelligence products, decision briefs and internal policies…[as well as] a selection of materials generated in support of these documents including emails and draft documents'.[8] The preliminary inquiry considered whether the classification decisions made were 'appropriate', as considered against five criteria. This included whether the decision was made in accordance with the PSPF, internal policy and procedure, source material and whether the decision maker was supported in their decision making.[9] The preliminary inquiry did not review the connection between classification decisions and the way that the PSPF is incorporated into the elements of offences in the *Criminal Code*.

---

5 *IGIS Act* (n 4) pt II div 3.

6 Inspector-General of Intelligence and Security, *2020-2021 Annual Report* (Report, 4 October 2021) 24; Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Inquiry into the Impact of the Exercise of Law Enforcement and Intelligence Powers on the Freedom of the Press* (Report, August 2020), recommendation 14.

7 Inspector-General of Intelligence and Security, *Preliminary Inquiry into the application of national security classifications in ASIO, ASIS, ONI, ASD, AGO and DIO* (Preliminary Report, 25 February 2021) 3 [11] ('*IGIS Preliminary Inquiry*').

8 *IGIS Preliminary Inquiry* (n 1) 7.

9 *IGIS Preliminary Inquiry* (n 1) 7.

The overall conclusion of the Inspector-General was that:

> *I am satisfied that there is no evidence to suggest there are systemic issues related to inappropriate classification of documents within the six intelligence agencies in my jurisdiction, and that an inquiry into this matter is not required at this time. This does not mean that every classification decision is perfect. There is always room for improvement and there are a number of staff who do not consider their training or guidance adequate or are unaware of agency guidance materials.*[10]

The comments about training and guidance were supported by the results of a survey conducted by IGIS that indicated:

- 30% of staff considered their training on making classification decisions to be inadequate.
- 20% said they were not aware of internal guidance or that it did not adequately equip them to make classification decisions.
- A majority relied on automated processes or procedures to guide decision and that for the most part this related to replying to emails.
- Emails were the most likely documents to be at risk of over classification.[11]

The Inspector-General made two recommendations relating to improving training and guidance material. The Inspector-General has not undertaken any dedicated inquiry or inspection work in follow-up to the preliminary inquiry but advised this review that the office has, 'on rare occasions, commented on such matters as part of inspections into specific agency operations'.[12] In that context the Inspector-General also noted that through that work they had seen no evidence of systemic over-classification.

The Law Council of Australia in its supplementary submission recommended that the Inspector-General conduct an updated review evaluating the implementation of its 2021 recommendations.[13] This is a matter for the Inspector-General.

10 *IGIS Preliminary Inquiry* (n 1) 8.
11 *IGIS Preliminary Inquiry* (n 1) 4-7.
12 Letter from Inspector-General of Intelligence and Security to INSLM, 21 February 2024.
13 Law Council of Australia, *Supplementary submission 26*, 11.