Australian Government
Attorney-General's Department
Security and Criminal Law Division

17/15685

13 February 2018

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
Parliament House
CANBERRA ACT 2600

Dear Committee Secretary

The Attorney-General's Department is pleased to provide a supplementary submission to the Committee's inquiry into the National Security Legislation Amendment (Espionage and Foreign Interference) Bill. I also attach the Attorney-General's Department's responses to the questions on notice from the public hearing on 31 January 2018 and the questions in writing received by the department on Friday 2 February.

This supplementary submission informs the Committee that the Attorney-General has asked the Department to progress the following changes to the general secrecy offences in Schedule 2 of the National Security Legislation Amendment (Espionage and Foreign Interference) Bill:

- improve the clarity of offences that apply to current and former Commonwealth officers, most particularly by narrowing the definitions of 'causes harm to Australia's interests' and 'inherently harmful information' at section 121.1 of the Bill
- creating separate offences that apply to non-Commonwealth officers that are narrower in scope than those applying to Commonwealth officers and only apply to the most serious and dangerous conduct, and
- strengthening the defence for journalists (at subsection 122.5(6)) by:
    - removing any requirement for journalists to demonstrate that their reporting was 'fair and accurate', ensuring that the defence is available where a journalist reasonably believes that their conduct was in the public interest, and
    - clarifying that the defence is available for editorial and support staff as well as journalists themselves.

The Government will shortly provide the Committee with a copy of the proposed Government amendments to the Bill.

The action officer for this matter is Tara Inverarity who can be contacted on [redacted]

Yours sincerely

Anna Harmer
First Assistant Secretary

PJCIS Inquiry into the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017

Attorney-General's Department Response to Questions on Notice and Questions in Writing

Questions on Notice

Question (page 34, Proof Transcript)

Senator FAWCETT: Is there a definition in this context for force and violence in terms of a threshold to be met?
Ms Inverarity: Sorry; I didn't bring the correct part of my Criminal Code to check the dictionary, but I do not believe—
Senator FAWCETT: You can take it on notice.
Ms Inverarity: Yes, I can take that on notice. I don't believe 'force' and 'violence' are defined. I think they take their ordinary meanings.

Answer

The terms 'force' and violence' are not defined in the *Criminal Code Act 1995* and take their ordinary meaning.

Question (page 41, Proof Transcript)

Mr DREYFUS: Could I ask you to take that question on notice and come back to the committee with information from the government about what inquiries or what investigations, if any, have been tasked by the government and, if they haven't, to tell us?

Answer

Consistent with longstanding practice, for reasons of national security, it is not appropriate to comment on intelligence or operational matters.

Questions in Writing

Could the Department please respond to concerns and recommendations raised in the following submissions and oral evidence:

Inquiry into the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017

- Human Rights Law Centre
- Law Council of Australia
- Joint Media Organisations
- Inspector-General of Intelligence and Security
- Commonwealth Ombudsman

- Australian Human Rights Commission
- Office of the Australian Information Commissioner

Submission 5 – Law Council of Australia

The Committee should await an assessment of the Bill for its impact on freedom of speech by the Parliamentary Joint Committee on Human Rights (PJCHR) before completing its inquiry and if necessary, extend the opportunity to make submissions in response to the information obtained. Any issues identified by the PJCHR should be addressed prior to enactment.

The department has no comment to make on the timing of the Committee's inquiry. The department is happy to consider any issues raised by PJCHR in its consideration of the Bill

The definition of 'national security' extending to the country's political or economic relations with another country or countries should be reconsidered.

In developing the definition of national security in section 90.4 of the Bill, the department considered other relevant definitions in other Commonwealth legislation. This included the definition of 'security' in section 4 of the ASIO Act and the definition of 'national security' in section 8 of the *National Security Information (Criminal and Civil Proceedings) Act 2004* (NSI Act).

Section 8 of the NSI Act defines national security to mean 'Australia's defence, security, international relations or law enforcement interests'. Section 9 of the NSI Act further defines 'security' to have the same meaning as in the ASIO Act. Section 10 of the NSI Act further defines 'international relations' to mean the political, military and economic relations with foreign governments and international organisations'.

The reference to 'political, military and economic relations' in section 90.4 of the Bill aligns with the definition of 'international relations' in the NSI Act.

The NSI Act substantially implemented the recommendations of the ALRC in *Keeping Secrets: The Protection of Classified and Security Sensitive Information* (Report 98, June 2004). This report recommended that 'national security information' be defined by reference to the Commonwealth Protective Security Manual that existed at that time, which included reference to 'international relations' in the same terms as appear in section 10 of the NSI Act (see paragraph 2.7 of the ALRC's Report).

The definition of 'national security' in proposed subsection 90.4(2) should define the terms 'espionage', 'sabotage', 'terrorism', 'political violence' and 'foreign interference'. The terms 'political violence' and 'foreign interference' should be defined in a manner consistent with section 4 of the *Australian Security Intelligence Organisation Act 1979* (Cth).

The definition of 'national security' needs to operate both in relation to Australia's national security and the national security of a foreign country.

The department is concerned that defining the terms 'espionage', 'sabotage', 'terrorism', 'political violence' and 'foreign interference' by reference to the meaning of these concepts in the Criminal

Code and other relevant Commonwealth legislation could limit the utility of the definition when considering the meaning of the national security of a foreign country.

A requirement should be inserted into proposed section 93.3 to indicate that a prosecution must not be initiated unless it has been certified by the Attorney-General that it is appropriate that the information concerned Australia's national security at the time of the conduct that is alleged to constitute the offence.

A certificate under section 93.3 is not intended to be compulsory. The Attorney-General may issue a certificate, which is prima facie evidence of the matters certified in it.If a certificate is not issued, the CDPP can seek to establish that the relevant information concerns national security by leading other evidence.

It would not be appropriate for section 93.3 to require the Attorney-General to issue a certificate in every matter. It is appropriate that the CDPP determine whether to seek a certificate from the Attorney-General, and for the Attorney-General to decide whether to issue it.

The department does not agree the Attorney-General should certify that it was 'appropriate' for the information to 'concern national security' at the time of the conduct constituting the offence. This is not an objective fact but rather a statement of opinion, which would not properly belong in an evidentiary certificate. The *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* states that evidentiary certificates are generally only suitable when they relate to formal or technical matters of fact that would be difficult to prove by adducing admissible evidence (at page 55).

Prosecution of the offences in Part 5.2 will require the consent of the Attorney-General, consistent with section 93.1.

Proposed section 93.3 should be amended to require the Attorney-General to only certify information or an article as concerning Australia's national security subject to the statutory criteria for 'national security'.

The Bill already achieves this effect. The definition of 'national security' will be inserted into Division 90, which sets out the definitions for Part 5.2 of the Criminal Code. Section 93.3 will be located in Part 5.2.Therefore, for the purposes of section 93.3, the Attorney-General will only be able to certify that information concerns 'national security' within the definition of the term in section 90.4

It is not clear whether the Attorney-General will be able to certify that the information or article concerns Australia's national security for the purposes of the sabotage offences. This should be clarified.

The evidentiary certificate provision in section 93.3 will only apply to the offences located in Part 5.2 of the Criminal Code.

It will not apply to the sabotage offences, which will be located in Part 5.1 of the Criminal Code.

In relation to the definition of 'public infrastructure', the Law Council considers that there would be benefit in a reference to the *Australian Government Information Security Manual 2016-2017*

(for example in the Explanatory Memorandum) and a need to be consistent with the requirements of that key policy document.

The definition of public infrastructure covers the infrastructure that is essential to Australia's defence or essential services, within the Commonwealth's constitutional power to legislate.

Systems that are covered by the controls within the scope of the Australian Government Information Security Manual are likely to be covered by paragraphs (a), (d) and (e) of the definition of 'public infrastructure'.

The department is not aware of how a reference to the Information Security Manual would assist in clarifying the scope of the definition of 'public infrastructure'.

The Explanatory Memorandum to the Bill should provide the demonstrated need to define 'security classified information' by prescription in the regulations.

The Explanatory Memorandum describes the justification for prescribing this definition in regulations at paragraph 588. These reasons include:

- the level of detail needed in the definition
- the changing nature of the subject matter
- the technicality of the definition, and
- the possible need to refer to treaty obligations.

The type of information which may be prescribed as 'security classified information' should be clearly defined and circumscribed in the Bill, for example, through appropriate criteria to assist in ensuring that the matter would, or would be reasonably likely to, cause harm to or prejudice Australia's national security.

The Explanatory Memorandum states (at paragraph 589) that it is anticipated that the regulations will prescribe the relevant protective markings that will denote information as being classified for the purpose of these offences. These protective markings are listed in the *Australian Government information security management guidelines – Australian Government security classification* system, available at www.protectivesecurity.gov.au.

Subsection 90.5(2) provides that the definition of 'security classified information' must not be inconsistent with the protective security policies of the Commonwealth.

A requirement similar to that which exists in section 50A of the *Australian Border Force Act 2017* (Cth) (the ABF Act) should be inserted into the Bill to indicate that a prosecution must not be initiated unless it has been certified that it is appropriate that the information had a security classification at the time of the conduct that is alleged to constitute the offence.

A certificate under section 93.3 is not intended to be compulsory. The Attorney-General may issue a certificate, which is prima facie evidence of the matters certified in it.

If a certificate is not issued, the CDPP will establish that the relevant information concerns national security by leading other evidence.

It would not be appropriate for section 93.3 to require the Attorney-General to issue a certificate in every matter. It is appropriate that the CDPP determine whether to seek a certificate from the Attorney-General, and for the Attorney-General to decide whether to issue it.

The department does not agree that the Attorney-General should certify that it was 'appropriate' for the information to 'concern national security' at the time of the conduct constituting the offence. This is not an objective fact but rather a statement of opinion, which does not properly belong in an evidentiary certificate.

The proposed definition of 'foreign intelligence agency' should be amended to mean (for example) an entity that is directed or controlled by a foreign government or governments that has responsibility for gathering security or defence intelligence about the capabilities, intentions or activities of people or organisations outside its own territory. If it is thought necessary to extend this definition to non-State actors, a reference could be made to a foreign political organisation. However, there must also be a link to Australia's national security in the offence provisions. More broadly, the definition of 'foreign intelligence' and 'foreign intelligence agency' should be reviewed to ensure consistency across Commonwealth legislation.

The department does not agree that it is necessary for the definition in the Bill to align with other legislative definitions of 'foreign intelligence agency' as the terms properly take different meaning in different contexts.

For example, the Law Council's submission refers to the definition of 'foreign intelligence agency' in the *Anti-Money Laundering and Counter Terrorism Financing Act 2006*. The definition in the AML-CTF Act relates to the ability of relevant agency heads to share information with foreign intelligence agencies, and in that context refers to Australian agencies charged with the collection of foreign intelligence. The purpose of the definition in the Criminal Code is to define a foreign entity in respect of which certain conduct will be a criminal offence.

A definition along the lines of an 'entity that is directed or controlled by a foreign government or governments that has responsibility for gathering security or defence intelligence about the capabilities, intentions or activities of people or organisations outside its own territory' would be more challenging to prove than the definition set out in the Bill and undermine the efficacy of the offences.

There is no intention to cover non-State actors in this definition. It is limited to agencies of foreign countries.

The proposed defences for public officials should not be available for sabotage, espionage and foreign interference offences under: proposed subparagraphs 82.3(1)(c)(i), 82.4(1)(c)(i), 82.5(1)(c)(i), 82.7(1)(d)(i) and (ii), 82.8(1)(d)(i) and (ii), 91.1(1)(c)(i), 91.1(2)(c)(i), 91.8(1)(b)(i), 91.8(2)(b)(i), 92.2(1)(c)(iv) and (d)(ii) and (d)(iii), 92.3(1)(c)(iv) and (d)(ii) and (d)(iii); and proposed subsections 91.2(1) and (2).

The Committee should inquire into the necessity to permit a public official defence for other sabotage, espionage and foreign interference offences where that conduct is engaged in on behalf of a foreign principal to advantage the national security of a foreign country. In the absence of such evidence, the proposed public officials defence should not proceed.

There are a range of scenarios in which these defences are appropriate, including where public officials are working with Australia's allies and partners for mutually beneficial outcomes.

For example, one of the functions of the Australian Secret Intelligence Service (ASIS) under paragraph 6(1)(d) of the *Intelligence Services Act 2001* is to liaise with intelligence or security services, or other authorities, of other countries. This can involve ASIS providing these agencies with security classified information, or information that concerns Australia's national security, with the intent of advantaging the national security of that foreign country—for example, by alerting the foreign country of an imminent risk of a terrorist act being committed within their territory or to assist the authorities of that country to locate persons (both Australians and other nationals) taken hostage by a terrorist organisation in that country. In these scenarios, the defences for public officials ensure that such conduct does not constitute an offence against section 91.1 (Espionage).

The proposed new treason offences should be limited to conduct that will materially assist the enemy to engage in armed conflict against the Commonwealth or the Australian Defence Force (ADF). Similarly, proposed section 80.1AB should provide that the Governor-General may, by Proclamation, declare a party (i.e a person, body or group of any kind) to be an enemy engaged in armed conflict against the Commonwealth or the ADF.

The submission proposes changing the word 'involving' to the word 'against' in the offence and in the Proclamation power.

This would not be appropriate given the realities of modern armed conflict. It is entirely possible that the ADF may be engaged in an armed conflict involving multiple actors such as insurgent groups. The ADF may not necessarily be engaged in combat operations against all of the actors in such a context. It may, for example, be engaged in training, advising, and otherwise assisting missions in support of and with the consent of a foreign government, which would not see Australia engaged in combat 'against' an enemy. In such circumstances, Australia may still be a party to the armed conflict, in which case the conduct intended to be caught by this provision should still be criminalised.

The department notes that the offence contains other elements that narrow the scope of the offence, including the requirement that the person provides 'material assistance'.

The Bill should prescribe certain criteria for when the Governor-General may make a Proclamation under proposed section 80.1AB.

Section 80.1AB allows the Governor-General to declare a party to be an enemy engaged in armed conflict involving the Commonwealth or the Australian Defence Force.

The department's view is that there would be no benefit in listing further criteria than are already contained in section 80.1AB. The question of whether a party is an enemy engaged in armed conflict

involving the Commonwealth or the Australian Defence Force will be determined based on expert advice in the context of the meaning of the terms in international law.

There should be a requirement of periodic review of such a Proclamation and an ability of revocation when the Governor-General is no longer satisfied that the criteria for making the Proclamation continues to be met.

The Proclamation will be a legislative instrument, which can be repealed through the usual processes.

In addition, legislative instruments sunset every 10 years under the operation of the *Legislation Act*, ensuring that such instruments are periodically reviewed and only re-made if required.

There should be a prohibition on the retrospective proclamation of a 'party to be an enemy engaged in armed conflict' under proposed section 80.1AB.

The *Legislation Act* prevents retrospective application of a Proclamation made under section 80.1AB of the Bill.

Consistent with subsection 12(2) of the *Legislation Act*, a legislative instrument does not apply in relation to a person if the provision commences before the day the instrument is registered, to the extent that as a result (a) the person's rights as at that day would be affected so as to disadvantage the person; or (b) liabilities would be imposed on the person in respect of anything done or omitted to be done before that day.

This replaces existing provisions in the Criminal Code which do allow for retrospective commencement of Proclamations. Consistent with existing subsections 80.1AA(2) and (2A) of the Criminal Code, a Proclamation may commence on the date that it is made, rather than the date on which it is registered.

The treachery offence in proposed 80.1AC should require the fault element of intention where the person engages in conduct involving the use of force or violence.

The prosecution will need to prove the physical element that the conduct involved force or violence and that the defendant was reckless as to this element. The prosecution will also need to prove that the person intentionally engaged in conduct.

As drafted, the physical element is a circumstance element. Consistent with section 5.6 of the Criminal Code, recklessness is the automatic fault element for a circumstance element. The *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement* Powers states (at page 20):

> The default fault elements were carefully considered and devised in the process of developing the Criminal Code. Consequently, the default fault elements supplied by the Criminal Code should apply unless there is a sound reason to depart from these.

The department has not identified a reason to override the automatic fault element and apply intention to this element.

The application of recklessness requires the prosecution to prove that the person was aware of a substantial risk that his or her conduct involved force or violence and that, having regard to the circumstances known to him or her, it was unjustifiable to take the risk.

In light of the Review of Commonwealth Criminal Law: Fifth Interim Report (the Gibbs Committee Report), the Law Council encourages the Committee to consider whether the broadening of the sabotage offences in the proposed manner is indeed necessary and justified.

The department considered a broad range of information and resources in developing the sabotage offences in the Bill. The goal was to develop appropriate sabotage offences for the modern age, which protect Australia's critical infrastructure from national security threats. In the modern environment, major telecommunications, electricity and gas networks are privately owned. The sabotage of such networks (whether privately or publicly owned) could gravely prejudice Australia's national security. An example is provided at paragraph 266 of the Explanatory Memorandum.

The department considered the Gibbs Review (from 1991) as well as the draft sabotage offence in the Model Criminal Code, developed jointly by all states, territories and the Commonwealth in 2001 through the Model Criminal Code Officers Committee of the Standing Committee of Attorneys-General.

These reports were prepared at a time prior to the inter-connected nature of public infrastructure, particularly since the development of the internet. The sabotage offences in the Bill have been developed in this context, and reflect the severe impacts on Australia's safety and security if such infrastructure is damaged or destroyed.

The extension of the sabotage offence provisions should be reconsidered. If this is not accepted by the Committee, the Law Council recommends that proposed subparagraphs 82.7(1)(d)(ii) and 82.8(d)(ii) of the Bill be amended to reflect the fact that the harm or prejudice to Australia's economic interests should be more than minor or trivial prejudice.

The offences of introducing vulnerabilities into public infrastructure (at sections 82.7 and 82.8 of the Bill) are necessary to prevent foreign and malicious actors from creating vulnerabilities in systems supporting Australia's public infrastructure.

These offences ensure that criminal sanctions apply where a person is implanting a vulnerability with the intention for it to later be exploited for the purposes of sabotage.

The usual meaning of 'harm' and 'prejudice' does not include minor or trivial matters and accordingly it is not necessary to amend the Bill to achieve this effect. This could be clarified in the Explanatory Memorandum, if the Committee considers that this would assist.

Proposed section 82.9 'Preparing for or planning sabotage offence' be removed from the Bill. Incitement, conspiracy and attempt provisions in Part 2.4 of the Criminal Code are sufficient to deal with preparatory conduct which has indicated a real intention to carry out the act. If this position is not accepted by the Committee, the Law Counsil recommends that there be a public review conducted by the Attorney-General's Department which clearly identifies the appropriate criteria which should be used for determining the kinds of criminal conduct that warrant

preparatory offences. The review should allow for a public submissions process and the outcomes be used to inform the *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* (the Guide).

The department disagrees that the extensions of criminal responsibility in Part 2.4 alone are sufficient in relation to sabotage offences. Preparatory offences in Commonwealth legislation are generally reserved for serious criminal conduct warranting criminalisation at the preparation stage.

This offence will give law enforcement authorities the means to deal with preparatory conduct, without the need to wait until a sabotage offence is attempted or committed putting essential public services at risk.

Liability for attempt arises from conduct that is 'more than merely preparatory' (subsection 11.1(2) of the Criminal Code). The proposed offence targets conduct that occurs before liability for attempt would arise. The preparatory offence criminalises conduct that would not yet amount to an attempt to commit a sabotage offence.

An offence of attempt carries the same penalty as the primary offence. In recognition of the nature of the preparatory offence, it carries a lower penalty than that applying to the primary sabotage offences.

The *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* provides general guidance on the matters to be considered when developing or amending criminal offences and enforcement powers. The Guide does not reflect a binding policy position but provides principles and precedents to assist the framing of criminal offences and related matters. The Guide draws its principles and precedents from Senate Committees and other sources, such as the Australian Law Reform Commission. Should the Committees express particular views regarding preparatory offences, consideration would be given to including guidance on these as well.

In the absence of sufficient justification to the contrary, a good faith defence should be available for the proposed sabotage offences.

A good faith defence is not considered appropriate.

The sabotage offences include elements requiring proof that the defendant intended (or was reckless as to whether his or conduct would) prejudice Australia's national security or advantage the national security of a foreign country. The department does not believe that these elements can be properly juxtaposed with a good faith defence. That is, the Department has been unable to identify circumstances in which sabotage of critical infrastructure being reckless as to the harm to Australia's interests could properly be said to be in good faith.

The proposed advocating mutiny offence should not proceed. Instead, an updated inciting mutiny offence should be created in the Criminal Code which replaces section 25 of the Crimes Act and is directed at serving ADF members or a defence force of another country that is acting in cooperation with the ADF. Incitement, conspiracy and attempt provisions in Part 2.4 of the Criminal Code are sufficient to deal with the offence of mutiny. If this is not to be accepted, the fault element of intention should apply as to whether the person's words of conduct will cause

another person to engage in mutiny. In addition, a good faith defence should be provided to ensure that individuals or groups who in good faith with oppose the actions of the ADF or a defence force of another country that is acting in cooperation with the ADF and/or calls for a laying down of arms is not subject to the offence.

The Law Council has suggested that the advocating mutiny offence be modelled on section 25 of the Crimes Act. This offence is outdated, archaic, and unusable, particularly since the enactment of extensions of criminal responsibility in Part 2.3 of the Criminal Code in 1995.

The new offence modernises existing section 25 and ensures that it appropriately complements the primary offence of mutiny in the *Defence Force Discipline Act* and the application of the extension of criminal responsibility of incitement at section 11.4 of the Criminal Code.

Mutiny is a serious offence with potentially serious consequences for the defence of Australia. Although civilians cannot commit the offence of mutiny, it is appropriate that criminal sanctions are available where civilians advocate defence members to engage in mutiny, reckless as to whether the result will be that a defence member will take part in a mutiny.

The Bill could be amended to provide that the good faith defence at section 80.3 of the Criminal Code is available for the offence of advocating mutiny. This would mean that the offence does not apply if a person engages in a limited range of conduct undertaken in good faith.

Consideration should be given to lowering the proposed penalty of 15 years imprisonment under proposed section 83.2 (assisting prisoners of war to escape) in light of the Third Geneva Convention which stipulates that a prisoner of war should not be punished for a successful escape, and that a prisoner of war captured in the process of escaping, if punished, should only be liable to a disciplinary punishment.

In respect of paragraphs 119 and 120 of the Law Council's submission, the element of the offence, which refers to the Third Geneva Convention, limits its reference to Article 4 of that Convention. The reference to the Third Geneva Convention is used only for the purposes of defining a prisoner of war, not for the interpretation of the offence generally.

The department acknowledges that there are relevant obligations in the Third Geneva Convention to ensure that prisoners of war are not subject to judicial punishment for escape, attempted escape or connected offences (Third Geneva Convention, Articles 91 – 93). These obligations require that a prisoner of war not be subject to anything more than disciplinary punishment for escape, attempted escape or connected offences (i.e. aiding or abetting an escape).

The offence at section 83.2 of the bill is not directed at the actions of prisoners of war themselves. Given that the offence does not criminalise the acts of prisoners of war but rather persons who assist prisoners of war to escape, it would not be appropriate for the penalty to be lowered based on the obligations in the Third Geneva Convention as the Law Council has suggested.

The proposed offence relating to military-style training involving a foreign government principal should be amended to reflect that it is only an offence for a person to undergo such training where

the person is specifically undergoing training for the execution of a predetermined hostile act and those training activities are an integral part of that hostile act.

The department does not agree that international humanitarian law is relevant to the interpretation of the offence in proposed section 83.3. International humanitarian law would only be relevant to the applicability and scope of the offence to the extent that the offence occurs during an armed conflict. Unlike other offences in the Bill, this offence is not linked to armed conflict.

The offence does not criminalise the direct participation of civilians in hostilities. This is a matter that is regulated by international humanitarian law, and in so far as war crimes, crimes against humanity and genocide are concerned, by Division 268 of the Criminal Code. Accordingly, the Law Council's comments on the scope of 'direct participation in active hostilities' are not relevant in these circumstances.

The policy basis for this offence is that there is an inherent threat to security when a foreign government is undertaking military-style training in Australia or training Australian citizens overseas, unless it is under a properly executed agreement with the Australian Government. This conduct poses a threat whether or not a specific hostile act is envisaged at the time.

An Australian domestic court is unable to make a finding against a foreign State under the principle of sovereignty at international law. Nonetheless, the Law Council encourages the Committee to inquire into the possible impact at international law as to whether a finding by an Australian court for the purposes of the proposed offence relating to military-style training involving a foreign government principal may amount to *opinio juris* at international law.

In relation to the Law Council's comments on issues of State Responsibility including the non-intervention principle at international law, these issues will not be relevant to a determination of individual criminal responsibility for the purposes of this offence.

Subparagraph 83.3(1)(c)(ii) will not require consideration of these international law issues and will not involve an Australian domestic court making a finding that a foreign State has violated the principle of non-interference, which in any event is not a determination an Australian domestic court is generally empowered to make. Such a determination would typically be a matter for an international court or tribunal.

A decision of an Australian court may constitute evidence of either State Practice or opinio juris, which are the two elements required to demonstrate the existence of a customary international law norm. In both instances, however, evidence of one country's practice or sense of obligation will be insufficient to demonstrate a rule of customary international law. There must be sufficiently widespread and representative practice among countries accompanied by a sense of legal obligation.

As noted above, the department's view is that a determination of guilt by Australian domestic court under proposed section 83.3 will not involve consideration of international law issues and in particular will not invoke or otherwise infringe on the non-intervention principle.

In relation to the interference with political rights and duties offence, the Explanatory Memorandum to the Bill should be amended to make clear that the availability of the offence does not affect the power of Parliament to deal with such conduct as contempt of Parliament, provided that a person may not be punished twice for the one act or omission.

Nothing in the Bill affects the Parliament's powers in relation to contempt. The department agrees with the Law Council that section 4C of the Crimes Act will operate to prevent double jeopardy.

Clear justification should be given for the maximum term of imprisonment and the increase by seven years for the interference with political rights and duties offence.

The right to engage in Australia's democratic and political processes is essential to Australia's free and open society. Conduct that not only interferes with these rights and but do so through the use of force, violence, intimidation or threats is an especially grave threat to Australia's democracy and stifles the open debate which is fundamental to Australia's society.

The espionage offences should not proceed

The expansion of the scope of the espionage offences is necessary in order to cover the full range of espionage conduct being engaged in by Australia's foreign adversaries.

The new offences criminalise a wider range of harmful conduct, and through that ensure that criminal investigation and prosecution are available to protect Australia's interests and prosecute perpetrators.

The new offences ensure that this harmful conduct is matched by serious criminal penalties to punish offenders, and deter potential offenders.

If this (the recommendation that the espionage offences should not proceed) is not accepted, the Law Council makes the following recommendations:

- **The proposed new espionage offences should regulate the dealing with 'Commonwealth information' which may be defined as information to which a person has, or had access by reason of his or her being, or having been, a Commonwealth officer or received from a Commonwealth officer.**

  The effect of this amendment would be to significantly limit the application of espionage offences only to Commonwealth officers and people who received information from a Commonwealth officer. This limitation is not present in existing offences relating to information about the Commonwealth's security and defence and its introduction undermine the protection of Australia's interests.

  The amendments seek to broaden the offences to cover the information being sought by Australia's foreign adversaries. Espionage activity is not limited to seeking information held by, or received from, a Commonwealth officer.

- **The proposed new espionage offences should require (as a minimum for 'outsiders') that the dealing with information did, or was reasonably likely to, or intended to prejudice Australia's national security or advantage the national security of a foreign country.**

  Existing espionage offences do not differentiate between 'insiders' and 'outsiders'. Under current law, any person can commit an espionage offence.

  The espionage offences proposed in the Bill will require proof that a person intended to, or was reckless as to whether his or her conduct would, prejudice Australia's national security. The most serious offences in section 91.1 also apply where a person intends to, or is reckless as to whether his or her conduct would advantage the national security of a foreign country.

  Proof of actual harm to Australia's national security or advantage to a foreign country's national security in the espionage offences would severely limit the scope of the offences and their effectiveness and require actual harm to occur before an offence arises. The harm addressed and criminalised by the espionage offence is the information being provided to a foreign power and the person's intention to prejudice Australia's national security or advantage the national security of a foreign country. The espionage offences in the Bill contain these elements.

- **In the absence of an express harm requirement, the offences should cascade in penalty and require that a person knew, or as a lesser offence, was reckless as to whether, the protected information falls within a particular category (i.e. security classification or concerns Australia's national security) and should not provide that strict liability applies to that circumstance.**

  The penalties for the espionage offences are tiered based on whether a person intended to, or was reckless as to whether, his or her conduct would prejudice Australia's national security or advantage the national security of a foreign country. Further tiering based on the person's level of knowledge about the nature of the information would not enhance the ability to relevantly discriminate across the seriousness of offending conduct.

  The effect of removing strict liability would be that the prosecution would need to prove that the defendant was reckless as to whether the information or article had a security classification. This would require proof that the person was aware of a substantial risk that the information or article carried a security classification and, having regard to the circumstances known to the person, it was unjustifiable to take that risk. Given the security classifications are prominently marked on documents, it is unnecessary to require proof of the fact of the classification.

- **Defences should be introduced to capture bona fide business dealings and persons acting in good faith. A defence should also be introduced for prior publication where the offences do not apply to a person dealing with the information if:**

  (a) the information has already been communicated, or made available, to the public (the *prior publication*); and

(b) the person was not involved in the prior publication (whether directly or indirectly); and

(c) at the time of the disclosure, the person believes that the disclosure:

(i) will not endanger the health or safety of any person; and

(ii) will not prejudice Australia's national security or advantage the national security of a foreign country; and

(d) the person has reasonable grounds for that belief.

A bona fide dealings or good faith defence is not appropriate in the context of espionage offences, which require proof of a person's intention or recklessness as to whether their conduct will prejudice Australia's national security or advantage the national security of a foreign country. The prosecution will be required to prove intention to prejudice Australia's security or recklessness thereto element beyond a reasonable doubt. It is difficult to conceive a situation in which a person could simultaneously be reckless as to harming Australia's national interest, yet be acting in good faith. Genuine good faith would preclude recklessness being made out.

In the case of espionage offences other than section 91.3, the prosecution will already have rebutted element (c)(ii) of the proposed defence in proving its case against the defendant.

- **Consideration should be given as to whether the proposed maximum penalties for the espionage offences which range between 15 years to life imprisonment are too high. The necessity of doubling the previous maximum term of seven years must be demonstrated to be necessary and proportionate.**

  The maximum penalty for existing espionage offences in section 91.1 of the Criminal Code is 25 years imprisonment, not seven years imprisonment as stated in the Law Council's submission.

  The Bill increases the maximum penalty for the most serious offence (in subsection 91.1(1)) to life imprisonment and applies tiered penalties to other offences in new Division 91.

A defence for persons acting in the public interest should be provided for the proposed foreign interference offences in Division 92, Subdivision B.

The foreign interference offences are characterised by conduct that influences Australia's political or governmental processes, interferes in Australia's democratic processes, supports the intelligence activities of a foreign principal or prejudices Australia's national security. The offences also require proof that the defendant's conduct was covert or deceptive, involved threats or menaces or targeted a person without disclosing the nature of the defendant's connection to a foreign principal.

In combination, this conduct poses threats to Australia's safety and security.

It is not clear that conduct constituting a foreign interference offence an be excused from criminal liability on the basis that it is 'in the public interest'. Conversely, conduct that it 'in the public interest' is unlikely to fall within the scope of the foreign interference offences in the Bill.

The preparing for a foreign interference offence in section 92.4 should not proceed. Instead, the ancillary provisions of the Criminal Code for incitement, conspiracy and attempt should be relied upon.

The department disagrees that the extensions of criminal responsibility in Part 2.4 alone are sufficient in relation to foreign interference offences. Preparatory offences in Commonwealth legislation are generally reserved for serious criminal conduct warranting criminalisation at the preparation stage.

This offence will give law enforcement authorities the means to deal with preparatory conduct, without the need to, for example, wait until a foreign interference offence is committed or an Australian process is put at risk of interference.

Liability for attempt arises from conduct that is 'more than merely preparatory' (subsection 11.1(2) of the Criminal Code). The proposed offence targets conduct that occurs before liability for attempt would arise. Conduct that amounted to an attempt to commit a foreign interference offence would not capture the range of conduct that the proposed offence would cover.

An offence of attempt carries the same penalty as the primary offence. In recognition of the nature of the preparatory offence, it carries a lower penalty than that applying to the primary foreign interference offences.

The proposed offences in sections 92.7 and 92.8 (relating to support for a foreign intelligence agency) should cascade in penalty and require that the person knew, or as a lesser offence, was reckless as to whether the support or resources would help the organisation to directly or indirectly engage in preparing, planning, assisting in or fostering an act prejudicial to Australia's security.

The department understands, from paragraph 163 of the Law Council's submission, that this suggestion is based on a comparison of the offences in sections 92.7 and 92.8 with the terrorist financing offences in Division 103 of Part 5.3 of the Criminal Code.

The policy basis of the offences in the Bill is that the provision of support to a foreign intelligence agency, in and of itself, presents a threat to Australia's national security.

The proposed new offences operate differently to the offences for financing terrorism in Division 103 of Part 5.3 of the Criminal Code and a more relevant comparison is the supporting terrorist organisation offences in sections 102.6 and 102.7 of the Criminal Code.

The inclusion of the element suggested by the Law Council would not support the policy intention of the offences, and would need to be matched with much higher penalties (for example, the offence of financing terrorism in section 103.1 of the Criminal Code carries a penalty of life imprisonment).

The proposed offences in sections 92.9 and 92.10 (relating to funding or being funded by a foreign intelligence agency) should require that the person is reckless as to whether the funds will be used to facilitate or engage in activities prejudicial to Australia's national security or, in the case of obtaining funds, involve undue influence.

The department does not consider that these elements are appropriate for inclusion in the offences in sections 92.9 and 92.10.

The policy basis of the offence is that the provision of funding to a foreign intelligence agency, in and of itself, presents a threat to Australia's national security.

The Explanatory Memorandum should clarify the intersection between the proposed foreign interference offences in the Bill and those in the Foreign Influence Transparency Scheme Bill 2017.

The offences in the Foreign Influence Transparency Bill 2017 complement the foreign interference offences in this Bill. The purpose of the offences is different – the foreign interference Bill criminalise conduct intended to cause harm to Australia's national security interests or advantaging another, whereas those in the transparency scheme support the enforcement of registration requirements.

Section 4C of the Crimes Act would prevent a person being prosecuted for both a FITS offence and a foreign interference offence.

The proposed offence of theft of trade secrets involving a foreign government principal should not proceed.

The Bill appropriately criminalises the theft of trade secrets where it is done on behalf of a foreign government principal. This amounts to economic espionage, which is harmful to Australia's national security and economic prosperity.

The Bill does not criminalise theft of trade secrets where a foreign government is not involved. This is properly left to civil enforcement mechanisms or state/territory theft offences.

The proposed general secrecy offences in the Bill should be amended in a manner which is consistent with the Australian Law Reform Commission's (ALRC) Report No 122, *Secrecy Laws and Open Government in Australia* (the Secrecy Report) and the Independent National Security Legislation Monitor's (the INSLM) report *Section 35P of the ASIO Act* (2016) (the ASIO Act Report).

Protecting Australia from espionage and foreign interference relies heavily on having strong protections for information, especially where disclosure causes harm to an essential public interest. The unauthorised disclosure or use of certain information can prejudice national security and defence or our relationships with foreign countries.

Criminal offences are necessary to deter such disclosures and punish them if they do occur.

The key premise of the ALRC's report was that secrecy offences should apply where the disclosure causes harm, is reasonably likely to cause harm or was intended to cause harm to an essential public interest.

The new secrecy offences are consistent with this view, although the Bill implements this in a different way to that envisaged by the ALRC.

The ALRC report is premised on the view that an express harm requirement should be proved. The Bill partially implements this approach in the offence of 'conduct causing harm to Australia's interests' in section 122.2. The ALRC accepted (in Chapter 8 of its report) that the disclosure of some categories of information could be inherently harmful, and that secrecy offences relating to the disclosure of such information would therefore not require an express harm element. This is reflected in the offence at 122.1, which does not require proof of an express harm requirement.

As noted in the department's supplementary submission, the Attorney-General has asked the department to progress changes to the Bill to create separate offences that apply to non-Commonwealth officers that are narrower in scope than those applying to Commonwealth officers and apply only to the most serious and dangerous conduct.

If this (amending the general secrecy offences consistent with the ALRC's Secrecy Report) is not to be accepted, the Law Council makes the below recommendations:

- **In the absence of an express harm requirement, the offences should cascade in penalty and require that a person knew, or as a lesser offence, was reckless as to whether, the protected information falls within a particular category (i.e. security classification or concerns national security), and should not provide that strict liability applies to that circumstance.**

  Other than for security classified information, the offences at sections 122.1 and 122.2 already require a person to be reckless as to the nature of the information (eg that it is 'inherently harmful information' or information the communication or dealing with which would cause harm to Australia's interests).

  In relation to security classified information, strict liability currently applies. The effect of removing strict liability would be that the prosecution would need to prove that the defendant was reckless as to whether the information or article had a security classification. This would require proof that the person was aware of a substantial risk that the information or article carried a security classification and, having regard to the circumstances known to the person, it was unjustifiable to take that risk.

  If the Committee considers it appropriate, the department would be open to the removal of strict liability from elements of the offences relating to information or articles carrying a security classification.

- **The secrecy of information offence provisions should be redrafted to treat insiders and outsiders separately to improve the proportionality of the measures.**

  Protecting Australia from espionage and foreign interference relies heavily on having strong protections for information, especially where disclosure causes harm to an essential public interest. The unauthorised disclosure or use of certain information can prejudice national security and defence or our relationships with foreign countries.

In the same way as any person can commit espionage, any person can threaten Australia's safety, security and stability through the unauthorised disclosure of harmful information.

As noted in the department's supplementary submission, the Attorney-General has asked the department to progress changes to the Bill to create separate offences that apply to non-Commonwealth officers that are narrower in scope than those applying to Commonwealth officers and apply only to the most serious and dangerous conduct.

- **The secrecy of information offence provisions should be redrafted to distinguish between intentional and reckless conduct regarding the communication or dealing with inherently harmful information or causing harm to Australia's interests.**

  The fault element of intention always applies to the physical elements of the secrecy offences involving conduct. Therefore, the prosecution will always have to prove that the person intentionally communicated or dealt with the information.

The phrase 'interfering with' should be removed from proposed paragraphs 121.1(a) and (b) of the Bill.

The department disagrees with this suggestion. It is important that the secrecy offences cover 'interference' with particular functions, rather than only 'prejudice' to those functions.

If the offences did not cover 'interference', the AFP would have to wait for a criminal investigation to actually be prejudiced before being able to investigate the matter as a secrecy offence. This creates risks to the Commonwealth that can be avoided if the AFP is able to intervene at an earlier stage, when the person's conduct is 'interfering with' (but has not yet actually prejudiced) a criminal investigation.

The phrase 'contravention of a provision, that is subject to a civil penalty, of' should be removed from proposed subparagraph 121.1(1)(a)(ii). As a minimum, the provision should be limited to contraventions of serious Commonwealth civil penalty provisions which attract an equivalent civil penalty of 3 years imprisonment.

The justification for the inclusion of civil penalties in the definition of 'causes harm to Australia's interests' is set out in paragraph 1284 of the Explanatory Memorandum.

As noted in the department's supplementary submission, the Attorney-General has asked the department to progress changes to the Bill to improve the clarity of offences that apply to current and former Commonwealth officers, most particularly by narrowing the definitions of 'causes harm to Australia's interests' and 'inherently harmful information' at section 121.1 of the Bill. The department will consider the inclusion of civil penalties in the definition of 'causes harm to Australia's interests' in that context.

The *Proceeds of Crime Act 2002* (Cth) (POCA) should be removed from proposed subparagraph 121.1(1)(b)(ii).

It is appropriate for the AFP's functions under the POCA to be covered in this definition. Strong action to confiscate proceeds of crime assists in attacking the profit motive of organised crime, and the effective performance of these functions is an essential public interest. The justification for the inclusion of the AFP's functions under the Proceeds of Crime Act in the definition of 'causes harm to Australia's interests' is set out in paragraphs 1288-1289 of the Explanatory Memorandum.

For the purposes of proposed paragraphs 121.1(d) and (e), the EM should clarify what may amount to 'intangible damage' and be amended to note a reduction in the '*quantity* or quality of information provided by a foreign government or international organisation.

The department notes the minor typographical error in paragraph 1298 of the Explanatory Memorandum where the word 'quality' should read 'quantity' and will correct the error in the re-printed Explanatory Memorandum.

The reference to 'intangible' damage to Australia's reputation or relationships is intended to cover situations where Australia's international standing is reduced in ways that are real, but not able to be specifically and individually listed. This is consistent with the ordinary meaning of the word.

The proposed 'inherently harmful information' criminal offences should not proceed in the absence of sound justification for the proposed categories, noting the previous consideration of the ALRC in its Secrecy Report.

The Explanatory Memorandum explains the justification for each category of information listed in the definition of 'inherently harmful information' from paragraph 1319 to paragraph 1333.

The categories of information covered by the definition are listed below:

- Security classified information: Assessments about the appropriate security classification are made by officers with the relevant knowledge and expertise in the subject-matter and context. For example, information should be classified as PROTECTED (the lowest of the security classifications) if the compromise of the confidentiality of information could be expected to cause damage to the national interest, organisation or individuals. A classification of TOP SECRET should be applied if the compromise of the confidentiality of information could be expected to cause exceptionally grave damage to the national interest. The application of a security classification therefore indicates that an appropriately qualified person has already made an assessment of the harmfulness of the information.

- Information the communication of which would, or could reasonably be expected to, damage the security or defence of Australia: This category of information is defined by reference to disclosures that would, or could reasonably be expected to, damage the security or defence of Australia. Therefore, the prosecution will have to prove this element beyond a reasonable doubt in order to establish the offence. This category of information is consistent with recommendation 5-1 of the ALRC's report.

- Information that was obtained by, or made by or on behalf of, a domestic or foreign intelligence agency in connection with the agency's functions: Information made or obtained by intelligence agencies carries inherent sensitivity. Information that may seem innocuous to a lay person can yield significant counterintelligence dividends to a foreign intelligence service. This category of information is consistent with the ALRC's discussion at paragraphs 8.33-8.72 of its report.

- Information that was provided to the Commonwealth in order to comply with an obligation under a law: This category of information is inherently harmful because it is essential that information that is provided to the Commonwealth under compulsion is protected. If this information is released, it will harm essential national interests by discouraging compliance with laws of the Commonwealth.

- Information relating to the operations, capabilities and technologies of, and methods and sources used by, a domestic or foreign law enforcement agency: Protection of sources is one of the most important obligations of law enforcement agencies. The consequences of disclosure of such information can be severe, including the death of the person acting as a source. The disclosure of information about operations, capabilities, technologies and methods is also highly sensitive. Disclosures of this information can prejudice the investigation of serious criminal activities and can allow criminals to evade the law.

Provisions relating to foreign intelligence agencies and foreign law enforcement agencies in the definition of 'inherently harmful information' should be redrafted to make it clear that the information would, or would be reasonably likely to, harm one of the four essential public interests identified by the ALRC in its Secrecy Report.

The department disagrees with this suggestion.

The Explanatory Memorandum, in particular paragraphs 1324-1326 (in relation to intelligence agency information) and paragraphs 1331-1332 (in relation to law enforcement information) of the Explanatory Memorandum, explains that such information is inherently harmful because of the adverse effect it can have on law enforcement and intelligence cooperation.

If foreign agencies share information with Australia, particularly about their most sensitive operations and techniques, it is essential that it can be appropriately protected. If this information-sharing were withdrawn, there would be significant adverse consequences for Australia's national interest.

If conduct relating to 'communication' continues to be regulated, proposed paragraph 121.1(b) of the definition of 'inherently harmful information' should be amended to read 'information to communication of which would, or would be reasonably likely to, damage the security or defence of Australia'.

The Law Council suggest changing 'could reasonably be expected to' to 'would be reasonably likely to' in paragraph (b) of the definition of inherently harmful information in section 121.1.

The department is not clear that the proposed change would make a material change to the definition.

The type of information which may be 'proper place of custody' should be more clearly defined and circumscribed in the Bill, for example, through appropriate criteria to assist in ensuring that the matter would, or would be reasonably likely to, cause harm to or prejudice Australia's national security.

The Explanatory Memorandum sets out the justification for 'proper place of custody' being defined in the regulations rather than the primary Act (see paragraph 1349).

In brief, these reasons are:

- the level of detail in the definition
- the changing nature of the subject matter
- the technical nature of the definition, and
- the definition may be determined by reference to treaty obligations.

The Explanatory Memorandum also explains that the definition is expected to cover buildings and other places of storage that are appropriate for information falling within the definition of 'inherently harmful information or 'causes harm to Australian interests', consistent with the Commonwealth's protective security policies.

The Committee consider whether the definition of 'Commonwealth officer' for the purposes of proposed subsection 121.1(1) should include the Governor-General.

The effect of expanding the definition of 'Commonwealth officer' would be twofold.

First, as suggested by the Law Council, it would allow information made or obtained by the Governor-General to be subject to the offences in sections 122.1 and 122.2.

Second, it would mean that the Governor-General could commit the offence at section 122.4 by communicating information that he or she was under a duty not to disclose (other than where a defence applies).

Schedule 2 of Part 1 of the Bill (Secrecy of information) should be amended to:

- **include a public interest disclosure defence to the secrecy provisions where the disclosure would, on balance, be in the public interest**

  There are established mechanisms for Commonwealth officers to make public interest disclosures under the Public Interest Disclosure Act. The inclusion of a public interest defence could disrupt the primacy of the Public Interest Disclosure Scheme as the mechanism for making disclosures of information.

- **non-exhaustively identify some factors that may be considered for the purposes of determining whether the dealing with or holding of information may be in the public interest for the purpose of the proposed journalist defence. Such factors may include for example:**

    - **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; and**

    - **revealing or substantiating that an agency (or a member of an agency) has engaged in misconduct or negligent, improper or unlawful conduct.**

  The Bill does not seek to define public interest beyond the exclusions listed in subsection 122.5(7). This allows the defendant to adduce or point to evidence that suggests a reasonable possibility that the person held or dealt with the information in the public interest (as required in order to discharge an evidential burden consistent with subsection 13.3(6) of the Criminal Code). Once this burden is discharged, the prosecution will then be required to prove the person did not hold or deal with the information in the public interest beyond reasonable doubt.

- **capture in proposed subsection 122.5(4) the dealing with information in order to make the communication in accordance with the *Public Interest Disclosure Act 2013* (Cth) (PID Act). the Committee should consider whether disclosures that may be made under private sector whistleblower laws under for example the Corporations Act 2001 (Cth) should also be captured by the defence provisions**

  The defence in subsection 122.5(4) could be broadened to cover other Commonwealth public interest disclosure schemes. The department notes however that neither it nor submissions have identified circumstances in which whistleblowers under other schemes would be dealing with inherently harmful information or information that causes harm to Australia's interests.

- **include an exception for where the conduct (i.e. communication/dealing with/holding/removing) is engaged in for the purpose of obtaining legal advice in relation to the matter the subject of the offence**

  It is not the intention to cover situations where a person is seeking legal advice about their ability to make a public interest disclosure or in relation to the application of the defences.

- **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**

  The existing defence at subsection 122.5(5) relating to provision of documents to a court or tribunal ensures that the offence does not criminalise making disclosures of information for the purposes of legal proceedings.

- **extend to where the person has dealt with or held the information (i.e. not just be limited to where they have communicated it) for the proposed defence relating to information that has previously been communicated, or made available, to the public. Similarly, the proposed defences relating to communication to an oversight body, information to a court or tribunal should extend to where the person has dealt with or held the information.**

  The department notes that the defences at subsections 122.5(3), (4), (5) and (8) do not explicitly extend to conduct involving dealings with information other than communications. The defences could be explicitly extended to cover a broader range of dealings.

  The department notes that, in relation to security classified information, there are significant risks attached to inappropriate storage or handling of such information. An extended defence would have the effect of not criminalising improper handling of highly classified information, leaving conduct that may be preparatory to more serious offences un-addressed.

- **insert an 'or' after paragraph 122.5(7)(c) and an 'and' after subparagraph 122.5(9)(d)(ii).**

  These appear to be minor drafting matters that will not affect the meaning of the provision. However, the department will raise these issues with the Office of Parliamentary Counsel to ensure that there are no unintended consequences of the omission of these words.

The defence to the proposed secrecy offences that permits disclosure with consent in section 47 of the Bill should be reconsidered.

The department believes that this comment relates to subparagraph 122.5(9)(d)(iii) of the Bill, as there is no section 47 in the Bill.

The defence in subsection 122.5(9) prevents the offences from applying to a person dealing in information that relates to them, or to limit the ability of a person to consent to another person dealing with information that relates to them. The Explanatory Memorandum provides examples of situations in which it is intended that the defence would ensure that a person is not inappropriately subject to criminal liability (see paragraph 1649).

The department believes this defence is necessary and prevents the criminal offences from operating too broadly, in situations where a person has consented to their information being dealt with, even if it is inherently harmful information.

A privacy impact assessment (PIA) should be conducted of the proposed secrecy provisions

The purpose of the general secrecy offences is, in part, to protect information the release of which would be harmful, including information that a person has been compelled to provide to the Commonwealth (see, for example, paragraph (d) of the definition of inherently harmful information). In this respect, the offences protect the privacy of individuals who provide information to the Commonwealth.

The proposed secrecy provisions should expressly indicate: whether they override the *Freedom of Information Act 1982* (Cth); and how they will interact with obligations under the *Privacy Act 1988* (Cth).

The offences will not apply if a person is acting within their duties (subsection 122.5(1)) or the information is made public with the authority of the Commonwealth (subsection 122.5(2)).

These defences will apply if a person is disclosing information under the Freedom of Information Act or Privacy Act in the proper performance of their functions.

The proposed aggravated offence for false and misleading conduct in proposed subsection 137.1A(1) should not proceed. Instead, it should be replaced with an offence of failing to disclose defined activities linked to a foreign country/principal in relation to an application for, or the maintenance of, an Australian Government security clearance. Alternatively, the aggravated offence for false and misleading information should be limited to activities linked to a foreign country/principal in relation to an application for, or the maintenance of, an Australian Government security clearance.

Security clearance processes are not only concerned with a person's foreign associations. They are intended to identify a range of potential vulnerabilities that may indicate that a person is not suitable to have access to classified information.

The provision of false or misleading information about a person's personal or financial circumstances can be just as important as the person's connections to a foreign country when determining a person's suitability to hold a security clearance.

Proposed subparagraph 5D(1)(e)(viii) (aggravated offence for giving false or misleading information) of the *Telecommunications (Interception and Access) Act 1979* (TIA Act) should be removed from the Bill so that this offence is not defined as a 'serious offence' for the purposes of the TIA Act. If this is not accepted by the Committee, the Law Council's recommendations regarding the improvement of this offence provision in accordance with the intent of the Bill becomes more acute.

The Explanatory Memorandum sets out the justification for telecommunications interception powers applying to this offence (see paragraph 1758). The use of telecommunications interception powers are likely to be critical in understanding a person's intentions, associations or other prejudicial activity, as well as the person's associations, in the context of the provision of false or misleading information as part of a security clearance process.

The presumption against the grant of bail under section 15AA Crimes Act should not be extended to treason, treachery, espionage and foreign interference cases as is proposed by the Bill.

The department does not agree with the Law Council's submission. The offences that are subject to a presumption against bail are very serious offences. The existing espionage, treason and treachery offences are currently listed in paragraph 15AA(2)(c) of the Crimes Act.

It is important to note that, consistent with subparagraphs 15AA(2)(c)(i) and (ii), the presumption against bail will only apply if the person's conduct is alleged to have caused the death of a person or carried a substantial risk of causing the death of a person.

The INSLM should review the bail and non-parole periods in sections 15AA and 19AG of the Crimes Act, including their impact on children.

The department notes this suggestion.

There should be no provision for a grant of bail to be stayed if the prosecution notifies an intention to appeal.

The department does not agree with the Law Council's submission. The offences that are subject to this provision (subsection 15AA(3C)) are very serious offences.

It is important to note that subsection 15AA(3C) will only apply if the person's conduct is alleged to have caused the death of a person or carried a substantial risk of causing the death of a person.

The department also notes that a grant of bail under s15AA can only be stayed for a maximum of 72 hours (see s15AA(3D)(c) of the Crimes Act).

The mandatory minimum non-parole period for terrorism offences, Division 80 (treachery, treason, urging violence and advocating terrorism or genocide) or 91 (offences relating to espionage and similar activities) under section 19AG should be repealed and not proceed.

The Bill does not amend section 19AG other than to remove an obsolete reference to the offence of treachery which is being repealed by the Bill.

Submission 8 - Commonwealth Ombudsman

Issue 1 – The introduction of new offences may impede our inspections functions and the ability of people to make complaints to my office

The Commonwealth Ombudsman's submission indicates that paragraphs (a) and (d) of the definition of 'inherently harmful information' in section 121.1 of the bill will cover information routinely sought by, or provided to, the Commonwealth Ombudsman during the course of investigations. The officers of the Commonwealth Ombudsman are potentially covered by the application of the secrecy offences.

The department agrees that staff of the Commonwealth Ombudsman will be covered by the new secrecy offences, as are all Commonwealth officers. This is consistent with existing section 70 of the Crimes Act, which applies to all Commonwealth officers.

The Commonwealth Ombudsman's submission also notes the existence of defences to provide relief to Commonwealth employees who breach the new offence provisions in the course of carrying out their duties and raises the policy question of whether Commonwealth officials should be covered by criminal offences in this situation. The submission raises the alternative policy option of the offences containing an element that the person was not acting in the course of their duties, to be proven by the prosecution.

The department considers it appropriate for the defendant to bear an evidential burden for pointing to evidence of how his or her conduct was authorised, either under law or as part of his or her duties. As set out at paragraph 1617 of the Explanatory Memorandum, the imposition of an evidential burden is appropriate because the defendant should be readily able to point to evidence that their conduct was either done in their official capacity as a Commonwealth officer. If this is done, the prosecution must refute the defence beyond reasonable doubt.

The Commonwealth Ombudsman's submission raises concerns that the defence at subsection 122.5(3) is too narrow. The submission states that the defence does not appear to be available for an offence under subsection 122.1(2) which relates to dealing with information. The defence would only be available if the information had actually been communicated to the Office of the Commonwealth Ombudsman and not if a person was dealing with the information (i.e.by photocopying a document) in order to communicate the information to the Office of the Commonwealth Ombudsman at a later date.

The defence at subsection 122.5(3) does not explicitly extend to conduct involving dealings with information other than communications. The defence could be explicitly extended to cover a broader range of dealings.

The department notes that, in relation to security classified information, there are significant risks attached to inappropriate storage or handling of such information. An extended defence would have the effect of not criminalising improper handling of highly classified information, leaving conduct that may be preparatory to more serious offences un-addressed.

Issue 2 – The interaction between the coercive powers provided by the Ombudsman Act and the new offence provisions may create a dilemma for agency staff

The Commonwealth Ombudsman's submission notes the existence of coercive powers in the *Ombudsman Act 1976* (Cth) that may require an agency staff member to produce information that is, or could be, inherently harmful information. Failure to comply with a request for information may result in an offence under the Ombudsman Act, which carries a significantly lower penalty than the new general secrecy offences. The submission indicates that agency staff members may find themselves in a dilemma about which piece of legislation has priority and resolve the problem by 'opting to transgress the provision with the lesser penalty', with the effect that information is not provided to the Commonwealth Ombudsman.

The department considers that a direction to provide information under section 9 of the Ombudsman Act would be effective where the disclosure would otherwise satisfy the elements of a general secrecy offence relating to the communication of information. The power in the Ombudsman Act is a specific power, available for limited purposes, which contemplates (in paragraph 9(4)(a)) that the provisions of an enactment, which would include a secrecy offence such as proposed subsection 122.1(1), do not excuse a person from complying with a section 9 requirement.

To the extent that there is any doubt, the department notes that a person providing information to the Ombudsman in accordance with a request under section 9 of the Ombudsman Act would have the benefit of the defences in subsections 122.5(1) and (3) of the Bill.

Issue 3 – The requirement to hold information at a 'proper place of custody'

The Commonwealth Ombudsman's submission notes that the Bill (and regulations) do not currently provide a definition of a proper place of custody. The submission raises concerns that the Office of the Commonwealth Ombudsman will hold inherently harmful information and, without a definition of proper place of custody, it is not clear what resourcing or other practical implications this requirement may have.

The department notes that most, if not all, Commonwealth departments and agencies will hold inherently harmful information. This information is already required to be stored and dealt with in accordance with the Commonwealth's protective security policies.

The definition of 'proper place of custody' will reflect the requirements of these protective security policies. There will be no additional burden on departments and agencies that are already complying with protective security policies.

The secrecy offences in the Bill are subject to delayed commencement and will commence by Proclamation, within six months of the Bill receiving the Royal Assent. The department intends to consult departments and agencies about the definition of proper place of custody during this period.

Issue 4 – The interaction between the new offences and the PID Act

The Commonwealth Ombudsman's submission notes that information communicated or dealt with in relation to a disclosure under the *Public Interest Disclosure Act 2013* (Cth) (PID Act) may fall within the definition of inherently harmful information. The submission notes that persons making disclosures in accordance with the PID Act, or Commonwealth employees who are tasked with functions under the PID Act, will need to rely on defences (in subsections 122.5(3) and (4)) to the general secrecy offences. The submission raises concerns about the limits of those defences in relation to dealings with information other than communications. The submission states that the Commonwealth Ombudsman foresees 'the possibility of these offences discouraging the making of disclosures, which is the purpose for which the PID Scheme was established' and raises the concern that Commonwealth employees could face uncertainty in the performance of their duties under the PID Act.

The defences at subsections 122.5(3) and (4) do not explicitly extend to conduct involving dealings with information other than communications. The defences could be explicitly extended to cover a broader range of dealings.

The department notes that, in relation to security classified information, there are significant risks attached to inappropriate storage or handling of such information. An extended defence would have the effect of not criminalising improper handling of highly classified information, leaving conduct that may be preparatory to more serious offences un-addressed.

Possible solution

The Commonwealth Ombudsman's submission proposes that a specific provision be included in the Criminal Code clarifying that Division 122 is not intended to override the immunities in section 24 of the PID Act and sections 7A, 8 and 9 of the Ombudsman Act.

The department continues to consider the interaction of the defences and immunities in light of the comments raised by in the submissions made by the Commonwealth Ombudsman and the IGIS. It may be possible to add a provision to Division 122 to make clear on the face of the Criminal Code that the enactment of the defences is not to be taken as reflecting an intention that they impliedly repeal or otherwise affect any other immunities.

Submission 9 – Joint Media Organisations

The proposed legislation criminalises all steps of news reporting, from gathering and researching of information to publication/communication, and applies criminal risk to journalists, other editorial staff and support staff that knows of the information that is now an offence to 'deal' with, hold and communicate.

The department does not agree with this assertion. Subsection 122.5(6) of the Bill creates a defence for an offence relating to the dealing with, or holding of, information if the person dealt with or held the information in the public interest in the person's capacity as a journalist engaged in fair and accurate reporting.

The defence does not however explicitly extend to the activities of editorial and other support staff, and could be expanded to explicitly deal with these matters.

We recommend that a general public interest/news reporting defence be available for all of the relevant provisions in both the secrecy and espionage elements of the bill

The department does not consider that espionage offences can be 'in the public interest'. It is hard to see how the passage of information to a foreign principal could be in the public interest where it is done with an intention to prejudice Australia's national security or advantage the national security of a foreign country.

The department notes that a defence specifically in relation to fair and accurate reporting in the public interest already exists in subsection 122.5(6) of the Bill. This addresses public interest news reporting.

The new offences apply to *all* persons, not just Commonwealth officers

Protecting Australia from espionage and foreign interference relies heavily on having strong protections for information, especially where disclosure causes harm to an essential public interest. The unauthorised disclosure or use of certain information can prejudice national security and defence or our relationships with foreign countries.

In the same way as any person can commit espionage, any person can threaten Australia's safety, security and stability through the unauthorised disclosure of harmful information.

As noted in the department's supplementary submission, the Attorney-General has asked the department to progress changes to the Bill to create separate offences that apply to non-Commonwealth officers that are narrower in scope than those applying to Commonwealth officers and only apply to the most serious and dangerous conduct.

'Deals' with information is unnecessarily broad – particularly when applied to the news media

The definition of 'deals' in section 90.1 of the Bill has been broadened to cover the full range of conduct that can constitute espionage and secrecy offences. This is to ensure the offences comprehensively deal with the full continuum of criminal behaviour is undertaken in the commission of espionage offences, and to allow authorities to intervene at any stage.

The department does not agree that receipt of information by a journalist would constitute a secrecy offence. Subsection 122.5(6) of the Bill creates a defence for an offence relating to the dealing with, or holding of, information if the person dealt with or held the information in the public interest in the person's capacity as a journalist engaged in fair and accurate reporting.

The department also does not agree that a person can 'automatically' breach any of the general secrecy offences. For an offence to be proved, the prosecution must establish each physical and fault element beyond a reasonable doubt. The prosecution would also have to rebut, beyond a reasonable doubt, any defences for which the defendant has discharged an evidential burden.

The forms of information are far broader than previously stated in legislation

The Bill adopts the existing definition of 'information' in section 90.1 of the Criminal Code. The Bill does not amend this definition.

The department agrees that existing secrecy offence in section 70 of the Crimes Act is currently limited to 'facts or documents' and that the application of the definition in section 90.1 will have the effect of broadening the application of the secrecy offences. It will ensure that the espionage and secrecy offences apply to information consistently.

The Explanatory Memorandum explains this at paragraphs 1315-1318.

Strict liability applies for communication or dealing in 'security classified information'

As stated in paragraph 1407 of the Explanatory Memorandum, strict liability has been applied because information or things carrying a security classification are clearly marked with the

classification and any person who has access to security classified information will be able to identify it as such.

The effect of removing strict liability would be that the prosecution would need to prove that the defendant was reckless as to whether the information or article had a security classification. This would require proof that the person was aware of a substantial risk that the information or article carried a security classification and, having regard to the circumstances known to the person, it was unjustifiable to take that risk.

Question whether paragraphs (d) and (e) of the definition of 'inherently harmful information' is excessive

The purpose of paragraph (e) of the definition of 'inherently harmful information', as set out at paragraph 1329 of the Explanatory Memorandum, is to protect information relating to the operations, capabilities, technologies, methods and sources of domestic or foreign law enforcement agencies. The disclosure of such information 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. A person will not be subject to criminal liability for communicating or otherwise dealing with information covered by paragraph (e) in circumstances covered by the defences in subsections 122.5(2) and (8), which deal with information that has previously been made public.

The purpose of paragraph (d) of the definition of 'inherently harmful information', as set out at paragraphs 1327-1328 of the Explanatory Memorandum, is to ensure that information provided to the Commonwealth under a coercive power or other compulsion is protected. If such information is not adequately protected, it could have the impact of discouraging individuals and companies from providing honest and complete information to the Commonwealth in accordance with an obligation under a law or otherwise by compulsion of law. However, there are likely to be a range of other secrecy provisions that protect such information and a Commonwealth officer is also likely to be under a duty not to disclose such information. As noted in the department's supplementary submission, the Attorney-General has asked the department to progress changes to the Bill to:

- create separate offences that apply to non-Commonwealth officers that are narrower in scope than those applying to Commonwealth officers and only apply to the most serious and dangerous conduct, and

- improve the clarity of offences that apply to current and former Commonwealth officers, most particularly by narrowing the definitions of 'causes harm to Australia's interests' and 'inherently harmful information' at section 121.1 of the Bill

A number of categories of information are excessive and/or unwarranted:

- **subparagraph (a)(ii), definition of 'cause harm to Australia's interests', section 121.1: civil penalty provisions**

  The department acknowledges that the inclusion of this category of information goes further than the ALRC's 2009 recommendation. The justification for the inclusion of this category of information is set out at paragraph 1284 of the Explanatory Memorandum.

  As noted in the department's supplementary submission, the Attorney-General has asked the department to progress changes to the Bill to improve the clarity of offences that apply to current and former Commonwealth officers, most particularly by narrowing the definitions of 'causes harm to Australia's interests' and 'inherently harmful information' at section 121.1 of the Bill

- **subparagraph (d), definition of 'cause harm to Australia's interests', section 121.1: harm international relations**

  The justification for this inclusion of this category of information is set out at paragraphs 1295-1298 of the Explanatory Memorandum.

  As noted in the department's supplementary submission, the Attorney-General has asked the department to progress changes to the Bill to improve the clarity of offences that apply to current and former Commonwealth officers, most particularly by narrowing the definitions of 'causes harm to Australia's interests' and 'inherently harmful information' at section 121.1 of the Bill

- **subparagraph (e), definition of 'cause harm to Australia's interests', section 121.1: Commonwealth-State relations**

  The department acknowledges that the inclusion of this category of information goes further than the ALRC's recommendation. The justification for the inclusion of this category of information is set out at paragraph 1300 of the Explanatory Memorandum.

  As noted in the department's supplementary submission, the Attorney-General has asked the department to progress changes to the Bill to improve the clarity of offences that apply to current and former Commonwealth officers, most particularly by narrowing the definitions of 'causes harm to Australia's interests' and 'inherently harmful information' at section 121.1 of the Bill

Section 122.4 – sunset provision on unauthorised disclosure of information by Commonwealth officers and former Commonwealth officers

As stated at paragraph 1589 of the Explanatory Memorandum, the offence in section 122.4 is intended to preserve the operation of specific duties that exist in other legislative frameworks until such time as each duty can be reviewed to determine whether it should be converted into a stand-alone specific secrecy offence, or whether criminal liability should be removed. Given the

number and diversity of such duties, this review is intended to be conducted as each duty is next considered, rather than within a time limited period. For this reason, the offence is not subject to a sunset provision.

Section 122.5 – defences – multiple issues that undermine the ability to report in the public interest:

- **subsection 122.5(2) – information that is already public**

  The secrecy offences contain two defences for information already in the public arena.

  The first defence (ss 122.5(2)) applies where information has been made public with the authority of the Commonwealth.

  The second defence (ss 122.5(8)) applies where a person (who did not make or obtain the information by being a Commonwealth officer) communicates information that has already been communicated by another person and the person reasonably believes that his/her communication will not cause harm to Australia's interests or the security or defence of Australia.

  These defences seek to strike a balance between freedom of expression on the one hand, and recognition that further dissemination of harmful information could cause additional harm on the other hand.

- **subsection 122.5(4) – information communicated in accordance with the *Public Interest Disclosure Act***

  The department has no comments on the adequacy of the PID Act.

- **subsection 122.5(6) – information dealt with or held for the purposes of fair and accurate reporting**

  The Explanatory Memorandum provides examples of how the activities of journalists in dealing with information may fall within the scope of the offences in Schedule 2 of the Bill. The department's view is that these paragraphs provide context for the operation of the defence. The department does not believe that these paragraphs in any way define or 'provide a framework' for the elements of public interest journalism. If there are material errors, the Explanatory Memorandum can be corrected.

  As described in the Explanatory Memorandum at paragraph 1639, the term 'journalist' is intended to take its ordinary meaning, leaving flexibility for a court to interpret the term consistent with the ordinary meaning at that particular time, which may not be the ordinary meaning of the term today. The Committee may wish to consider whether the inclusion of an exhaustive definition of journalist in the Criminal Code is desirable, which would then require amendment in future if the concept of the term 'journalist' evolves or changes.

As noted in the department's supplementary submission, the Attorney-General has asked the department to progress changes to the Bill to strengthen the defence for journalists (at subsection 122.5(6)) by removing any requirement for journalists to demonstrate that their reporting was 'fair and accurate', ensuring that the defence is available where a journalist reasonably believes that their conduct was in the public interest, and clarifying that the defence is available for editorial and support staff as well as journalists themselves.

The defence at subsection 122.5(6) is focused on the nature of the reporting, not the source of the information. The relevance of the source to this defence is not immediately clear to the department.

The department notes that a PJCIS review of the operation of the Data Retention Regime under the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015,* including the journalist information warrant scheme, must commence on or before 13 April 2019. .

- **subsection 122.5(8) – information that has been previously communicated**

  This defence seeks to strike a balance between freedom of expression on the one hand, and recognition that further dissemination of harmful information could cause additional harm on the other hand. Before disclosing information that has already been published, a person must believe on reasonable grounds that the subsequent disclosure will not cause harm. This is because in some cases, even where information is considered to have been published and in the public domain, subsequent disclosure will still result in harm. An example of this is provided at paragraph 1646 of the Explanatory Memorandum.

The offences carry substantially longer penalties and there is a very real risk of jailing journalists

The general secrecy offences are not intended to target journalists performing their ordinary work, as evidenced by the defence in 122.5(6).

As noted in the department's supplementary submission, the Attorney-General has asked the department to progress changes to the Bill to:

- create separate offences that apply to non-Commonwealth officers that are narrower in scope than those applying to Commonwealth officers and only apply to the most serious and dangerous conduct, and

- strengthen the defence for journalists (at subsection 122.5(6)) by removing any requirement for journalists to demonstrate that their reporting was 'fair and accurate', ensuring that the defence is available where a journalist reasonably believes that their conduct was in the public interest, and clarifying that the defence is available for editorial and support staff as well as journalists themselves.

Section 91.1 – dealing with information etc concerning national security which is or will be available to a foreign power

Although it is possible that the information could be communicated to a foreign principal through publication of news, the offence in section 91.1 can only be established if the person was aware of a substantial risk that his or her conduct would prejudice Australia's national security or advantage the national security of a foreign country and, having regard to the circumstances known to him or her, it is unjustifiable to take the risk (paragraph 91.2(2)(b)).

If these elements are proved beyond a reasonable doubt, the department does not see a policy basis for providing a defence for journalists to this offence.

Sections 92.7 and 92.8 – foreign interference involving foreign intelligence agencies

The department's view is that this submission reads too much into the word 'supports'. The Explanatory Memorandum states, at paragraph 1061, that what constitutes support will depend on the facts of each case but would extend to assistance in the form of providing a benefit or other practical goods and materials, as well as engaging in conduct intended to aid, assist or enhance an organisation's activities, operations or objectives.

The department notes that the offences require the person committing the offence to intend to provide support to an organisation that the person knows, or is reckless as to whether the organisation is, a foreign intelligence agency.

Submission 11 – Human Rights Law Centre

Criminal offences for the disclosure of information should only be introduced where the particular disclosure caused harm, or was intended to cause harm, to an essential public interest, such as the security and defence of Australia

The key premise of the ALRC's report was that secrecy offences should apply where the disclosure causes harm, is reasonably likely to cause harm or was intended to cause harm to an essential public interest.

The ALRC report is premised on the view that an express harm requirement should be proved. The Bill gives effect to this approach in part through the offence of 'conduct causing harm to Australia's interests' in section 122.2. The new secrecy offence at section 122.2 is consistent with this view, although the Bill implements this in a different way to that envisaged by the ALRC.

The ALRC also recognised that the disclosures of certain categories of information, such as information obtained or generated by intelligence agencies, would be inherently harmful, and considered that it would not be necessary to include a separate harm element in such cases. The offence at 122.1 deals with a limited range of categories of inherently harmful information, and does not contain an express harm element.

As noted in the department's supplementary submission, the Attorney-General has asked the department to progress changes to the Bill to create separate offences that apply to

non-Commonwealth officers that are narrower in scope than those applying to Commonwealth officers and only apply to the most serious and dangerous conduct.

The Bill includes an offence (in new section 122.4) that is substantially similar to the outdated section 70 of the Crimes Act

As stated at paragraph 1589 of the Explanatory Memorandum, the offence in section 122.4 is intended to preserve the operation of specific duties that exist in other legislative frameworks until such time as each duty can be reviewed to determine whether it should be converted into a stand-alone specific secrecy offence, or whether criminal liability should be removed. Given the number and diversity of such duties, this review is intended to be conducted as each duty is next considered, rather than within a limited period.

Where the Bill does adopt a harm-based approach, it extends protection beyond essential public interests to other interests which are appropriately protected by administrative and employment obligations, <u>not</u> serious criminal offences

The definition of 'causes harm to Australia's interests' aligns in part with the recommendations of the ALRC. As set out in paragraph 1282 of the Explanatory Memorandum, paragraphs (a), (c), (d) and (f)[1] of the definition correspond with the categories of harm recommended by the ALRC.

In relation to the other paragraphs of the definition, the Explanatory Memorandum sets out the reasons for the inclusion of additional categories:

- the justification for subparagraph (a)(ii), relating to civil penalties, is at paragraph 1284 of the Explanatory Memorandum
- the justification for paragraph (b), regarding certain functions of the AFP, is at paragraphs 1286-1289 of the Explanatory Memorandum, and
- the justification for paragraph (e), regarding relations between the Commonwealth and a State or Territory, is at paragraph 1300 of the Explanatory Memorandum.

As noted in the department's supplementary submission, the Attorney-General has asked the department to progress changes to the Bill to improve the clarity of offences that apply to current and former Commonwealth officers, most particularly by narrowing the definitions of 'causes harm to Australia's interests' and 'inherently harmful information' at section 121.1 of the Bill.

[1] There is a minor error in the Explanatory Memorandum which refers to paragraph (g) instead of paragraph (f).

The proposed criminal offences extend to an excessive breadth of information, including:

- **information to which the public may have a right of access under freedom of information laws)**

  The secrecy offences are subject to a defence for persons acting within their powers, functions and duties as a Commonwealth officer. This would include release of information under freedom of information laws.

- **types of conduct (including mere possession of information)**

  The definition of 'deals' in section 90.1 of the Bill has been broadened to cover the full range of conduct that can constitute espionage and secrecy offences. This is to ensure the offences comprehensively deal with the full continuum of criminal behaviour that are undertaken in the commission of espionage offences, and to allow authorities to intervene at any stage.

  The fault element of intention will apply to the physical element of the offence that a person communicates or deals with information.

- **to all persons**

  Protecting Australia from espionage and foreign interference relies heavily on having strong protections for information, especially where disclosure causes harm to an essential public interest. The unauthorised disclosure or use of certain information can prejudice national security and defence or our relationships with foreign countries.

  In the same way as any person can commit espionage, any person can threaten Australia's safety, security and stability through the unauthorised disclosure of harmful information.

  As noted in the department's supplementary submission, the Attorney-General has asked the department to progress changes to the Bill to create separate offences that apply to non-Commonwealth officers that are narrower in scope than those applying to Commonwealth officers and only apply to the most serious and dangerous conduct.

The Bill does not sufficiently protect whistleblowers acting in the public interest, with the excessive breadth of the new offences creating several gaps between the protection available in the *Public Interest Disclosure Act 2013* and the defences available in Schedule 2

There are established mechanisms for Commonwealth officers to make public interest disclosures under the Public Interest Disclosure Act. The inclusion of a general public interest defence would disrupt the primacy of the Public Interest Disclosure Scheme as the mechanism for making disclosures of information.

The defence at subsection 122.5(4) could be explicitly extended to cover a broader range of dealings.

The Bill dramatically increases penalties from the current law, again contrary to the recommendations of the ALRC, to some of the most severe terms of imprisonment available under

Australian law. This raises serious risk of a chilling effect that extends beyond the conduct covered by the offences to lawful communications about government. It would serve to intimidate public servants rather than encourage a culture of open government

Commonwealth criminal law policy, as set out in the *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*, is that each offence should have a single maximum penalty that is adequate to deter or punish a worst case offence, including repeat offences. The maximum penalty should aim to provide an effective deterrent to the commission of the offence, and should reflect the seriousness of the offence within the relevant legislative scheme.

In the case of the secrecy offences, the disclosure of information falling within the definitions of 'inherently harmful information' or information that does, will or is likely to 'cause harm to Australia's interests' could, as a worst case scenario, lead to loss of life.

In light of this worst case scenario, the maximum penalties are considered appropriate.

The Bill's reliance on internal security classification of documents as the basis for general criminal offences is wholly inappropriate

The justification for the inclusion of security classified information as a category of inherently harmful information is included in the Explanatory Memorandum at paragraphs 1321-1322.

Assessments about the appropriate security classification are made by officers with the relevant knowledge and expertise in the subject-matter and context. For example, a classification of TOP SECRET should be applied if the compromise of the confidentiality of information could be expected to cause exceptionally grave damage to the national interest. The application of a security classification therefore indicates that an appropriately qualified person has made an assessment of the harmfulness of the information.

There are appropriate processes for reviewing a security classification and determining whether it remains appropriate. These processes should be followed in all cases where a person believes that security classified information should no longer have a security classification. Accordingly, the communication (or other dealing) with information that is security classified – either following a review that has determined that the information remains security classified, or where the classification has not been reviewed by a person who is familiar with the underlying reasons for its classification – will, or would reasonably be expected to, cause harm to the Commonwealth or an individual and warrants criminal liability.

Submission 13 – Inspector-General of Intelligence and Security

The defences to the new 'dealing' and 'removal' offences require proof of communication

It may not be sufficiently clear whether the defence at subsection 122.5(3) extends to conduct involving dealings with information other than communications. The defence could be explicitly extended to cover a broader range of dealings.

The department notes that, in relation to security classified information, there are significant risks attached to inappropriate storage or handling of such information.

New offences may override existing immunity provisions in the IGIS Act and PID Act

The department continues to consider the interaction of the defences and immunities in light of the comments raised by in the submissions made by the Commonwealth Ombudsman and the IGIS. It may be possible to add a provision to Division 122 to make clear on the face of the Criminal Code that the enactment of the defences is not to be taken as reflecting an intention that they impliedly repeal or otherwise affect any other immunities.

The need for IGIS officials to rely on a defence to a serious offence to undertake their normal duties

The department considers it is appropriate for a defendant to bear an evidential burden for pointing to evidence of how his or her conduct was authorised, either under law or as part of his or her duties, noting that IGIS officials are in a unique position in relation to their ability to discharge an evidential burden (addressed below). As set out at paragraph 1617 of the Explanatory Memorandum, the imposition of an evidential burden is appropriate for non-IGIS officials because the defendant should be readily able to point to evidence that their conduct was done in their official capacity as a Commonwealth officer. Where such evidence is identified, the prosecution must refute the defence beyond reasonable doubt.

The department notes that other secrecy offences are structured similarly, see for example section 35P of the ASIO Act, which provides an exception for IGIS officials in paragraph 35P(3)(g).

Inability of IGIS officials to discharge an evidential burden as part of the defence to an offence under Division 122

The department notes the IGIS's submission about the challenges faced by IGIS officials in discharging an evidentiary burden. Consistent with the proposed solution in the submission, a provision similar to section 18D of the ASIO Act could be included in the Bill to ensure that IGIS officials do not bear an evidential burden for the defences in Schedule 2.

No direct link between the proposed concepts of 'sabotage', 'espionage' and 'foreign interference' in the Criminal Code and existing concepts in the definition of 'security' in the ASIO Act

The department does not consider it appropriate for the scope of ASIO's functions to be limited by reference to the meaning of certain terms in the criminal law. This is not consistent with ASIO's functions as a security intelligence service.

The focus of criminal offences is on the acts of an individual. While ASIO has an interest in the acts of individuals, it is more broadly concerned with the activities of foreign powers, and the systemic use of espionage, sabotage or foreign interference as it relates to those powers. To link the definitions to the ASIO Act may have the unintended consequence of limiting the scope of ASIO's powers.

Provisions concerning the security classification of information

Section 90.5 of the Bill provides for 'security classification' to have the meaning prescribed in the regulations. As described at paragraph 588 of the Explanatory Memorandum, it is appropriate to prescribe the meaning of this term in the regulations because:

- the definition will involve a level of detail and technicality that is not appropriate for a principal Act
- the definition is expected to change regularly to keep up to date with changes in Commonwealth protective security policy
- elements of the definition may be determined by reference to treaties in order to comply with Australia's international obligations.

The department continues to consider the interaction of the defences and immunities in light of the comments raised by in the submissions made by the Commonwealth Ombudsman and the IGIS. It may be possible to add a provision to Division 122 to make clear on the face of the Criminal Code that the enactment of the defences is not to be taken as reflecting an intention that they impliedly repeal or otherwise affect any other immunities.

Section 90.5(2) requires the Minister to be satisfied that the regulations are not inconsistent with the policies of the Government of the Commonwealth in relation to protective security.

There is no intention to allow for documents that are not publicly available to be incorporated into the definition, as indicated by the reference in the Explanatory Memorandum to the Commonwealth's protective security policies being publicly available on the internet. This requirement (that any documents incorporated into the definition must be publicly available) could be specifically set out in section 90.5.

Offence of failing to comply with a lawful direction regarding inherently harmful information

The department's view is that when a person is dealing with the type of harmful information that is covered by the offences in Schedule 2, it is important that lawful directions about the retention, use or disposal of the information are complied with. The department does not agree with the assertion that breach of such directions are necessarily 'relatively trivial', when taking into account the nature of the information covered by the offences.

The onus will be on the prosecution to prove, beyond a reasonable doubt, that there was a lawful direction. The prosecution will also have to prove that the defendant was reckless as to this element.

As noted in the department's supplementary submission, the Attorney-General has asked the department to progress changes to the Bill to create separate offences that apply to non-Commonwealth officers that are narrower in scope than those applying to Commonwealth officers and only apply to the most serious and dangerous conduct.

Submission 16 – Office of the Australian Information Commissioner

Additional information should be included in the Explanatory Memorandum to explain how the expanded definition of 'serious offence' in the *Telecommunications (Interception and Access) Act 1979* is reasonable, necessary and proportionate, given the likely impact of this expanded definition on individuals' privacy

The department's view is that the inclusion of secrecy offences and aggravated false and misleading information offence in the definition of serious offence under the TIA Act is reasonable, necessary and proportionate.

The offences in the Bill target conduct which supports espionage and foreign interference activities seeking to cause great harm to Australia's national security. It is appropriate that law enforcement agencies can take reasonable steps to detect and investigate such conduct, given the serious consequences the activities may have for Australia's national security.

The Explanatory Memorandum provides detailed justification for the inclusion of all of the relevant offences in the definition of 'serious offence' in the TIA Act, from paragraph 1743 to 1762.

A note should be included in the Bill, or additional information included in the Explanatory Memorandum to the Bill, to clarify that the secrecy provisions are not intended to impact on Australian Privacy Principle 12 and the Privacy Act, including the Notifiable Data Breaches scheme

The department's view is that the secrecy offences do not override these provisions. Indeed, these provisions may be an example of the types of requirements that would indicate that a person's activities were authorised by law or part of their duties (for the purposes of the defences in section 122.5).

This could be clarified in the Explanatory Memorandum.

Submission 17 – Australian Human Rights Commission

The secrecy provisions in Schedule 2 do not, for the most part, distinguish between conduct engaged in by 'insiders' and by 'outsiders'

Protecting Australia from espionage and foreign interference relies heavily on having strong protections for information, especially where disclosure causes harm to an essential public interest. The unauthorised disclosure or use of certain information can prejudice national security and defence or our relationships with foreign countries.

In the same way as any person can commit espionage, any person can threaten Australia's safety, security and stability through the unauthorised disclosure of harmful information.

As noted in the department's supplementary submission, the Attorney-General has asked the department to progress changes to the Bill to create separate offences that apply to non-Commonwealth officers that are narrower in scope than those applying to Commonwealth officers and only apply to the most serious and dangerous conduct.

The secrecy provisions in Schedule 2 are not limited to prohibiting disclosures that are shown to damage the interests of the Commonwealth

The Explanatory Memorandum explains the justification for each category of information listed in the definition of 'inherently harmful information' from paragraph 1319 to paragraph 1333.

The categories of information covered by the definition are listed below:

- Security classified information: Assessments about the appropriate security classification are made by officers with the relevant knowledge and expertise in the subject-matter and context. For example, a classification of TOP SECRET should be applied if the compromise of the confidentiality of information could be expected to cause exceptionally grave damage to the national interest. The application of a security classification therefore indicates that an appropriately qualified person has already made an assessment of the harmfulness of the information.

- Information the communication of which would, or could reasonably be expected to, damage the security or defence of Australia: This category of information is defined by reference to disclosures that would, or could reasonably be expected to, damage the security or defence of Australia. The prosecution will have to prove this element beyond a reasonable doubt in order to establish the offence. This category of information is consistent with recommendation 5-1 of the ALRC's report.

- Information that was obtained by, or made by or on behalf of, a domestic or foreign intelligence agency in connection with the agency's functions: Information made or obtained by intelligence agencies carries inherent sensitivity. Information that may seem innocuous to a lay person can yield significant counterintelligence dividends to a foreign intelligence service. This category of information is consistent with paragraphs 8.33-8.72 of the ALRC's report.

- Information that was provided to the Commonwealth in order to comply with an obligation under a law: This category of information is inherently harmful because it is essential that information that is provided to the Commonwealth under compulsion is protected. If this information is released, it will harm essential national interests by discouraging compliance with laws of the Commonwealth.

- Information relating to the operations, capabilities and technologies of, and methods and sources used by, a domestic or foreign law enforcement agency: Protection of sources is one of the most important obligations of law enforcement agencies. The consequences of disclosure of such information can be severe, including the death of the person acting as a source. The disclosure of information about operations, capabilities, technologies and methods is also highly sensitive. Disclosures of this information can prejudice the investigation of serious criminal activities and can allow criminals to evade the law.

The categories of information covered by the definition of 'causes harm to Australia's interests' all require proof of harm to, interference with, or prejudice to, one of the listed categories. These reflect essential public interests

The secrecy offences in Schedule 2 contain inappropriate strict liability provisions

The effect of removing strict liability would be that the prosecution would need to prove that the defendant was reckless as to whether the information or article had a security classification. This would require proof that the person was aware of a substantial risk that the information or article carried a security classification and, having regard to the circumstances known to the person, it was unjustifiable to take that risk.

The secrecy offences in Schedule 2 do not contain adequate defences:

- **the defence relating to information that is 'already public' only applies where the prior publication was authorised by the Commonwealth**

  The secrecy offences contain two defences for information already in the public arena.

  The first defence (ss 122.5(2)) applies where information has been made public with the authority of the Commonwealth.

  The second defence (ss 122.5(8)) applies where a person (who did not make or obtain the information by being a Commonwealth officer) communicates information that has already been communicated by another person and the person reasonably believes that his/her communication will not cause harm to Australia's interests or the security or defence of Australia.

  These defences seek to strike a balance between freedom of expression on the one hand, and recognition that further dissemination of harmful information could cause additional harm on the other hand.

- **the defence in proposed subsection 122.5(8) applies only to *communications* made by an 'outsider' of information that has already been communicated. The defence does not apply to outsiders who *deal* with such information**

  The defence at subsection 122.5(8) does not explicitly extend to conduct involving dealings with information other than communications. The defence could be explicitly extended to cover a broader range of dealings.

  The department notes that, in relation to security classified information, there are significant risks attached to inappropriate storage or handling of such information.

- **while there is a defence for journalists, there is no general defence for whistleblowers who made disclosures that are in the public interest**

  There are established mechanisms for Commonwealth officers to make public interest disclosures under the Public Interest Disclosure Act. The inclusion of a public interest

defence could disrupt the primacy of the Public Interest Disclosure Scheme as the mechanism for making disclosures of information.

Questions in writing

Rationale for the Bill

1. *What process was undertaken by the Attorney-General's Department to develop the new legislation? What organisations were consulted?*

In May 2017, the Prime Minister requested that the former Attorney-General undertake a comprehensive review of Australia's espionage and foreign interference laws.

To undertake the Review, the Attorney-General's Department established a taskforce comprised of officers from the department and secondees from the Australian Security Intelligence Organisation and the Australian Federal Police. The Commonwealth Director of Public Prosecutions was closely involved in the work of the Taskforce.

The Review was overseen by an Advisory Group, chaired by the Attorney-General's Department, comprised of senior representatives from the following departments and agencies:

- Australian Electoral Commission
- Australian Federal Police
- Australian Secret Intelligence Service
- Australian Signals Directorate
- Australian Security Intelligence Organisation
- Australian Taxation Office
- Commonwealth Director of Public Prosecutions
- Department of Defence
- Department of Finance
- Department of Foreign Affairs and Trade
- Department of Immigration and Border Protection
- Department of the Prime Minister and Cabinet

The above agencies were consulted on the proposed reforms. The department also undertook general consultation with international counterparts, including:

- US Department of Justice

- Federal Bureau of Investigation
- US Attorney's Office
- Office of the Director of National Intelligence
- Canadian Department of Justice
- Royal Canadian Mounted Police
- Canadian Secret Intelligence Service

The department consulted departments and agencies affected by consequential amendments in the Bill and the Office of Parliamentary Counsel undertook the usual scrutiny consultation on the Bills in accordance with its drafting directions.

Definition of 'national security'

2. Why does the definition of 'national security' extend to political and economic relationships?

In developing the definition of national security in section 90.4 of the Bill, the department considered other relevant definitions in other Commonwealth legislation. This included the definition of 'security' in section 4 of the ASIO Act and the definition of 'national security' in section 8 of the *National Security Information (Criminal and Civil Proceedings) Act 2004* (NSI Act).

Section 8 of the NSI Act defines national security to mean 'Australia's defence, security, international relations or law enforcement interests'. Section 9 of the NSI Act further defines 'security' to have the same meaning as in the ASIO Act. Section 10 of the NSI Act further defines 'international relations' to mean the political, military and economic relations with foreign governments and international organisations'.

The reference to 'political, military and economic relations' in section 90.4 of the Bill aligns with the definition of 'international relations' in the NSI Act. The department notes that the ALRC recommended that, in the context of secrecy offences, the terms 'security' and 'international relations' should be defined by reference to the relevant provisions of the ASIO Act and the NSI Act in its 2009 report *Secrecy Laws and Open Government in Australia.*

The NSI Act substantially implemented the recommendations of the ALRC in *Keeping Secrets: The Protection of Classified and Security Sensitive Information* (Report 98, June 2004). This report recommended that 'national security information' be defined by reference to the Commonwealth Protective Security Manual that existed at that time, which included reference to 'international relations' in the same terms as appear in section 10 of the NSI Act (see paragraph 2.7 of the ALRC's Report).

The department's view is that the reference to 'political and economic relationships' could include such matters as:

- information-sharing between governments, including in relation to negotiating positions, strategic outlooks and agency information

- the confidence or trust held by one government in another government
- the ability of a government to maintain good working relations with a foreign government
- a government's reputation or relationships with a foreign government, or between officials

3. *What is intended to be covered by the term 'political, military or economic relations' in the definition of 'national security'? Could these terms be further clarified in the Bill or Explanatory Memorandum?*

The term is intended to have the same effect as it has in the definition in the NSI Act and to apply broadly to all aspects of a country's relationships with another country in relation to political, military and economic matters.

This covers foreign relations and foreign policy, including a country's strategies for dealing with other nations. It would cover the issues, strategies and methods by which a country seeks to advance its national interests, including with allies, or to protect itself from threats. It would extend to matters involving the country's economic interests, including international negotiations or agreements that may advance a country's economic interests.

The concept of 'international relations' is described in the Explanatory Memorandum, in the context of the secrecy offences, in paragraph 1298. The ALRC also considered the meaning of this term in its 2009 report, *Secrecy Laws and Open Government in Australia*, from paragraph 5.43 to 5.46.

4. *Could this broad definition of national security result in espionage or foreign interference allegations against a person who advocates against a particular trade agreement or military alliance? How is freedom of political expression protected?*

Although it is difficult to provide definitive advice about hypothetical scenarios, the department does not consider that these matters would fall within the scope of the espionage and foreign interference offences.

For example, in relation to the espionage offences, the offence will only be committed if a person deals with information with an intention to (or reckless as to whether his or her conduct will) prejudice Australia's national security. If the information the person is dealing with concerns national security or is security classified, the offence will also apply if the person intends to (or is reckless as to whether his or her conduct will) advantage the national security of a foreign country. The Explanatory Memorandum clarifies the meaning of 'prejudice' and 'advantage' at paragraphs 615 and 616.

Circular references in definition of 'national security'

5. *The offences in the Bill for sabotage, espionage and foreign interference include the term 'national security'. The term 'national security' is defined in the Bill to include activities in relation to 'sabotage', 'espionage' and 'foreign interference'. Do these circular references make it unclear exactly what is being criminalised?*

The department does not believe that these are circular references when taken in the context of the whole definition of 'national security' and its use in the offences.

Paragraph 90.4(1)(b) provides that 'national security' means the protection of a country from activities covered by subsection 90.4(2). The term 'national security' therefore means the protection of the country from espionage, sabotage, terrorism, political violence and other activities aimed at hindering the defence of the country,

In the context of subparagraph 91.1(b)(ii), the application of the definition in section 90.4 means that a person will be dealing with information 'concerning national security' if the information relates to a country's ability to protect itself from, for example, terrorism. In the context of subparagraph 91.1(c)(i), the application of the definition in section 90.4 means that a person will intend to prejudice 'Australia's national security' if the person intends to prejudice Australia's ability to protect itself from terrorism.

6. *In relation to Australia's national security, what does*

   (a) the term 'sabotage' in the definition of 'national security' mean?

   (b) the term 'espionage' in the definition of 'national security' mean?

   (c) the term 'foreign interference' in the definition of 'national security' mean?

The definition in section 90.4 defines the term 'national security' both for the purpose of Australia's national security and the national security of a foreign country. For this reason, the terms listed in subsection 90.4(2) are not limited by reference to Australia's laws as this may be unnecessarily limiting when the definition is used in the context of determining the meaning of 'the national security of a foreign country'.

In the context of Australia's national security, it is possible that a court would interpret the terms set out in Question 6 as being limited to the meaning of the terms as implemented in the offences of the Criminal Code. However, a court may wish to consider a broader interpretation if the ordinary or dictionary meaning is more expansive than the scope of the offences in the Criminal Code.

The department considers that it should be open to a court to find that these terms should be interpreted as broadly as is appropriate, based on the admissible evidence.

7. *In relation to foreign countries, is it intended that the terms sabotage, espionage and foreign interference will take their meaning from the criminal or other laws of the foreign country?*

The definition in section 90.4 defines the term 'national security' both for the purpose of Australia's national security and the national security of a foreign country. For this reason, the terms listed in subsection 90.4(2) are not limited by reference to Australia's laws as this may be unnecessarily limiting when the definition is used in the context of determining the meaning of 'the national security of a foreign country'.

The department considers that it should be open to a court to interpret these terms broadly in relation to the 'national security of a foreign country', based on the admissible evidence.

'Advantage the national security of a foreign country'

8. *Isn't it possible to 'advantage the national security of a foreign country', for example one of Australia's allies, without detrimentally affecting Australia's national security? Shouldn't the conduct the Bill seeks to deter only be that conduct that detrimentally affects Australia's national security?*

If a person is advantaging the national security of one of Australia's allies, the defence at subsection 91.4(1) would apply.

The department notes that, to this extent this is an issue, it would also be an issue with the existing espionage offences. The structure of the existing offence at subsection 91.1(2) of the Criminal Code has been replicated, with the exception of casting the matter of 'lawful authority' as a defence rather than as an element of the offence.

'Prejudice Australia's national security'

9. *Given the descriptor of 'prejudice', is this proportionate to the maximum penalties for sabotage, espionage and foreign interference offences?*

The term 'prejudice' appears in the existing espionage and sabotage offences, which carry serious penalties.

As set out at paragraph 615 of the Explanatory Memorandum, the term 'prejudice' is intended to capture a broad range of conduct including an intention to harm or injure Australia's national security or to cause disadvantage to Australia. It is intended to cover impairment or loss to Australia's national security interests.

The department considers that this conduct is very serious, and is proportionate to the maximum penalties that appear in the Bill, which have been tiered to match the seriousness of the relevant offences.

10. *Could the offences be tiered to distinguish between prejudice which is more than trivial, and prejudice which is 'substantial' or serious?*

Commonwealth criminal law policy, as set out in the *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*, is that each offence should have a single maximum

penalty that is adequate to deter or punish a worst case offence, including repeat offences. The maximum penalty should aim to provide an effective deterrent to the commission of the offence, and should reflect the seriousness of the offence within the relevant legislative scheme.

The department's view is that the maximum penalties for each of the offences in the Bill appropriately reflect the 'worst case scenario' for that offence. A sentencing court will clearly have the discretion to set the penalty at an appropriate level to reflect the relative seriousness of the offence based on the facts and circumstances of the particular case.

11. *Will 'embarrassment' ever constitute prejudice? For example, could 'embarrassment' caused to the Australian government be considered prejudicial to Australia's political, economic or military relations?*

Paragraph 615 of the Explanatory Memorandum states that 'the prejudice to Australia's national security is not required to be serious or substantial but is intended to be more than a minor or trivial prejudice that has no long-lasting effect, nor embarrassment to an Australian person or Australia's people'.

In the context of international relations, the ALRC made the following comments in paragraph 5.45 of its 2009 report, *Secrecy Laws and Open Government in Australia*:

> A disclosure that embarrasses the Australian Government may also cause damage to Australia's international relations. For example, where a disclosure damaged Australia's reputation, as well as being 'embarrassing', it may lead to a loss of confidence or trust in Australia. A loss of confidence in the Australian Government's capacity to protect information is likely to result in a restricted flow of information from foreign governments. This, in turn, may impact on Australia's capacity to protect national security or on Australia's capacity to function in the global political, military and economic environment.

Expanded grounds for in-camera proceedings

12. *Will amending the threshold in section 93.2 of the Criminal Code from the 'interest of the security or defence of the Commonwealth', to the 'interests of Australia's national security' increase the number of proceedings which could be held in camera? If so, how will the amendment impact the principles of open justice?*

The term 'security or defence' is not exhaustively defined in the Criminal Code. The scope of the term is unknown, as the espionage offences have not been prosecuted. It is therefore not possible to know whether the term would be interpreted more narrowly than the new definition of 'national security' in section 90.4.

Section 93.2 complements any available state and territory laws allowing for suppression orders or non-publication orders to be imposed on national security grounds (such the *Open Courts Act 2013* (Vic) and the *Court Suppression and Non-Publication Orders Act 2010* (NSW)). Section 93.2 provides a power to appropriately manage proceedings where the court is satisfied that it is in the interests of Australia's national security to do so. This is an important protection and the decision as to whether to exercise the power remains with the court.

It is not possible to determine whether this will have an effect on how many proceedings which could be held in camera. This decision is properly a matter for the court. The amendment ensures the alignment of this provision with the new definitions proposed to be inserted by the Bill.

The department notes that the CDPP's Guidelines and Directions Manual, which is available publicly at www.cdpp.gov.au, has a chapter on suppression orders, which provides guidance on where a suppression order will be sought by the CDPP. This guidance material states that the CDPP should only seek a suppression order for the furtherance of, or otherwise in the interests of, the administration of justice and when satisfied that special circumstances exist which require a suppression order to be made. Such circumstances include where the publication of evidence or information may endanger the national or international security of Australia.

13. What impact could this amendment have on the media's ability to report court proceedings?

The media will be subject to whatever orders a court considers necessary, in the interests of Australia's national security. The decision of a court to grant an order and the nature of the court's orders, rather than section 93.2 itself, will determine the media's ability to report on proceedings.

Interaction between the Bill and ASIO's mandate

14. What practical impact, if any, will the Bill have on the interpretation of the definition of 'security' within the ASIO Act?

This Bill will not have any practical impact on the interpretation of the definition of 'security' within the ASIO Act.

The interpretation of the definition of 'security' is not directly affected by the Bill, which makes no amendments to the ASIO Act.

ASIO is a security intelligence agency, responsible for obtaining, correlating and evaluating intelligence relevant to security. ASIO is not a law enforcement agency and is not responsible for investigating or prosecuting criminal offences. Accordingly, ASIO's functions should not be construed by reference to the criminal law. Amendments to the criminal law in this Bill should, therefore, not affect the interpretation of the ASIO Act.

15. Will the proposed broadening of espionage, sabotage and foreign interference create any uncertainty regarding ASIO's legislative mandate? Will the Bill expand ASIO's powers?

See answer to Question 14.

16. ASIO has made submissions to the Committee's review of its questioning and detention powers, proposing an expansion of those powers to all heads of security in the ASIO Act, including espionage, sabotage and foreign interference. What might be the impact of the amendments in this Bill on the availability of those powers to ASIO?

This Bill does not affect ASIO's questioning and questioning and detention warrants

Currently, ASIO's questioning and detention warrants are limited to matters related to terrorism offences. This Bill will not affect terrorism offences.

ASIO is a security intelligence agency, responsible for obtaining, correlating and evaluating intelligence relevant to security. ASIO is not a law enforcement agency and is not responsible for investigating or prosecuting criminal offences. Accordingly, ASIO's functions should not be construed by reference to the criminal law. Amendments to the criminal law in this Bill should, therefore, not affect the interpretation of the ASIO Act.

17. Is the definition of 'foreign interference' in the ASIO Act consistent with the offences proposed by the Bill? Does the definition in the ASIO Act need to be amended?

The department considered the definition of 'acts of foreign interference' in the ASIO Act as part of the policy development process. The department also considered overseas offences targeting agents of foreign powers, particularly in the United States Code.

The offences in the Bill are intended to criminalise harmful conduct and ensure criminal penalties can be applied to such conduct. This affects the functions of the AFP and CDPP as criminal investigative and prosecution agencies.

ASIO has distinct functions as a security intelligence service. It is not necessary for the definition of 'acts of foreign interference' in the ASIO Act to be consistent with the offences proposed in the Bill.

Definition of 'foreign principal'

18. Why are different definitions of 'foreign principal' used in the FITS Bill and the EFI Bill?

Different definitions are used to reflect the very different purposes and policy goals of the two Bills.

It would not be appropriate for the definition of 'foreign principal' for the purposes of the serious criminal offences in this Bill to be as broad as the definition for the FITS Bill, which aims to bring transparency to foreign influence in Australia's political and governmental processes.

It would be inappropriate, for example, to extend espionage offences to conduct undertaken on behalf of a foreign business or foreign individual. These offences are limited to conduct undertaken on behalf of foreign countries and a limited range of non-state actors.

19. Why does the definition under the EFI Bill extend to entities that are 'owned, directed or controlled' by foreign public enterprises, local or regional government bodies or foreign political organisations?

The definition extends to entities that are 'owned, directed or controlled' by other foreign principals to ensure that there are no gaps in coverage that can be exploited by Australia's foreign adversaries. If the definition did not cover these entities, it would be very easy for a foreign principal to avoid the application of the offences by simply, for example, running their espionage activities through another company that the entity owns or controls.

If it is accepted that foreign public enterprises, local or regional government bodies and foreign political organisations should fall within the definition of 'foreign principal', the department's view is that there is no policy reason why the definition should not also extend to entities that are owned, directed or controlled by these foreign principals.

20. The FITS Bill adopts an approach of treating foreign principals that are 'close to' a foreign government differently to foreign principals that are more distanced. Why has a similar approach not been adopted in the EFI Bill.

A similar approach has been taken in this Bill.

For example, the offences at section 83.3 (military-style training involving foreign government principal) and section 92A.1 (theft of trade secrets involving foreign government principal) only apply where the foreign principal is a foreign government principal.

For other offences, it is not considered appropriate to differentiate between conduct undertaken on behalf of a foreign government principal or any other category of foreign principal.

Reversal of the onus of proof

21. Why do the proposed new espionage, secrecy, sabotage and foreign interference offences place the evidential burden on the defendant to prove that their conduct was legitimate?

The justification for casting the matter of 'lawful authority' as a defence is dealt with in the Explanatory Memorandum in the discussion of each offence. For example, in relation to the defences for espionage offences in section 91.4, paragraphs 709-710 of the Explanatory Memorandum states:

> Lawful authority is currently included as a physical element of some of the existing espionage offences in Division 91 of the Criminal Code where a person communicates, or makes available, information intending to give an advantage [to] another country's security or defence (for example, subparagraph 91.1(2)(b)(i)). This requires the prosecution to prove, beyond a reasonable doubt, that the person did not have lawful authority for their actions. In contrast, subsection 91.4(1) casts the matter of lawful authority as a defence, which has the effect of placing an evidential burden on the defendant.
>
> If lawful authority was an element of the espionage offences in Subdivision A, it would be necessary for the prosecution to prove, beyond a reasonable doubt, that there was no authority in any law or in any aspect of the person's duties that authorised the person to deal with the information or article in the relevant manner. This is a significant barrier to prosecutions.
>
> It is appropriate for the matter of lawful authority to be cast as a defence because the source of the alleged authority for the defendant's actions is peculiarly within the defendant's knowledge. It is significantly more cost-effective for the defendant to assert this matter rather than the prosecution needing to disprove the existence of any authority, from any source.

The department further notes that the defence of lawful authority in section 10.5 applies to all Commonwealth offences. If a person wished to assert this defence in relation to any Commonwealth offence, that person would bear the evidential burden for doing so.

a. What sort of evidence would the defendant need to put forward to discharge the evidential burden

This will vary depending on the source of the alleged authority. In some cases, the authority may arise from a law of the Commonwealth or an agreement that the Commonwealth has

with another country. In this situation, the defendant may point to or adduce evidence of these matters. This can also include pointing to matters within the evidence adduced by the prosecution.

Subsection 13.3(6) of the Criminal Code defines 'evidential burden' to mean 'the burden of adducing or pointing to evidence that suggests a reasonable possibility that the matter exists or does not exist.' In *R v Khazaal* (2012) 246 CLR 601, the High Court at [74] accepted that it was right to contend that the words 'adducing or pointing to evidence that suggests a reasonable possibility' which appear subsection 13.3(6) of the Criminal Code, required no more than 'slender evidence' in relation to the issue of the relevant negative state of affairs that arose in that case. The High Court also held that, in determining whether the burden created by subsection 13.3(6) had been discharged, 'the evidence may be taken at its most favourable to the accused'.

It is also noted that in practice, the prosecution will have regard to any lines of defence which are plainly open on the evidence or have been indicated by an alleged accused when making a determination that there are reasonable prospects of conviction and that the matter should proceed.

b. Could there be circumstances in which a defendant was unable to produce evidence that their dealing with certain information was lawful, for example because it was only authorised under a verbal agreement.

Oral evidence as to the existence of an agreement may be sufficient to discharge the evidential burden.

22. In relation to Commonwealth public servants, why is the question of whether a person communicated (or dealt with) classified information in the course of their official duties considered to be 'peculiarly within the knowledge of the defendant'? Wouldn't the person's employer be best placed to have this knowledge.

The department does not agree that this is correct. It is not possible for an employer to put themselves in the shoes of the employee who dealt with the information to determine why they thought their particular action was lawful. This is especially the case where a person's dealing with the information falls outside those established by any legal framework or administrative practice known to the employer.

If the onus is on the prosecution to prove beyond a reasonable doubt that there was no authority, it will have to negative the fact that there was authority for the person's actions in any law, or in any aspect of the person's duty or in any of the instructions given by the person's supervisors (at any level).

Conversely, if a Commonwealth officer had a particular reason for thinking that they were acting in accordance with a law or with their duties, it should not be hard to them to describe where they thought that authority arose. The onus would then be on the prosecution to disprove the existence of that particular authority, beyond a reasonable doubt.

23. *Will the majority of conduct captured by the secrecy and espionage offences (ignoring the available defences) be legitimately undertaken by staff of Government departments or agencies?*

    a. *Isn't the question of whether or not information was communicated (or dealt with) in the course of a person's official duties central to the question of culpability for the offence?*

    b. *Why shouldn't the onus be on the prosecution to establish that, at a minimum, the conduct engaged in was not part of the person's official duties?*

The department does not agree that it makes sense to consider the offences 'ignoring the available defences'. The defences are an integral part of the overall offence framework and the offences cannot be properly construed if the defences are not taken into account.

The question of why the onus should not be on the prosecution is answered above at Question 21.

In some ways, the inclusion of the defence at, for example, section 91.4 increases the protections available to defendants. The existing espionage offence at subsection 91.1(1) does not require the prosecution to prove that the person acted without lawful authority, nor does it provide a defence similar to that introduced in the Bill at section 91.4. A defendant would have to rely on the general defence of lawful authority at section 10.5 of the Criminal Code, which is narrower than the new defences in section 91.4.

Key elements of espionage and secrecy offences prescribed in regulations

24. *Why is the term 'security classification' proposed to be defined in regulations, rather than in the Bill (see proposed s. 90.5)? Please provide a copy of the draft regulations and/or an overview of its contents, if any.*

The justification for the inclusion of the definition of 'security classification' in the regulations is set out at paragraphs 588-590 of the Explanatory Memorandum, extracted below:

> It is necessary to prescribe the meaning of the term security classification in the regulations for the following reasons.
>
> - The definition will involve a level of detail that is not appropriate for inclusion in the Criminal Code. The definition may prescribe specific words and protective markings that indicated that a document or article carries a security classification.
>
> - Prescription in regulations is necessary because of the changing nature of the subject matter. It will be necessary for the definition to keep up to date with changes to Commonwealth protective security policy, to ensure that there is no inconsistency between that which the policy requires or authorises, and that which is subject to the offence provisions;
>
> - The relevant material involves material of such a technical nature that it is not appropriate to deal with it in the Criminal Code.
>
> - Elements of the offence may be determined by reference to treaties in order to comply with Australia's international obligations. Australia concludes treaties and international agreements for the handling of certain information, such as classified information received from or given to

foreign governments, which may be relevant to the definition of a security classification in relation to such information.

It is anticipated that the regulations will prescribe the relevant protective markings that will denote information as being classified for the purpose of these offences. At this time, these markings are listed in the Australian Government information security management guidelines – Australian Government security classification system (available at www.protectivesecurity.gov.au) and include:

- PROTECTED
- CONFIDENTIAL
- SECRET
- TOP SECRET

Subsection 90.5(2) requires that, before the Governor-General makes regulations for the purposes of subsection 90.5(1), the Minister must be satisfied that the regulations are not inconsistent with the policies of the Government of the Commonwealth in relation to protective security. The intention is to allow the protective markings set out in the Protective Security Policy Framework to be reproduced in the regulations and kept updated in accordance with any changes to that Framework.

Draft regulations have not yet been developed.

As noted in the department's supplementary submission, the Attorney-General has asked the department to progress changes to the Bill to improve the clarity of secrecy offences that apply to current and former Commonwealth officers, most particularly by narrowing the definitions of 'causes harm to Australia's interests' and 'inherently harmful information' at section 121.1 of the Bill. The department will consider the appropriateness of the current definition of 'security classification in this context.

An alternative approach would be to specify the relevant markings (such as TOP SECRET and SECRET) in the Criminal Code, and allow only *equivalent* classifications to be prescribed in the regulations.

25. *What levels of classification are intended to be included in these regulations? Would the Bill as currently drafted allow low level markings, such as 'for official use only' to attract criminal sanction?*

Noting the answer to Question 24, the classifications to be included in any regulations would be a matter for the Government.

26. *Noting that the information covered in the secrecy offence will not always be in the form of a written document, is it appropriate for strict liability to apply to elements of the offences concerning security classification?*

Articles that carry a security classification are also marked with an appropriate security classification marker.

The effect of removing strict liability would be that the prosecution would need to prove that the defendant was reckless as to whether the information or article had a security classification. This

would require proof that the person was aware of a substantial risk that the information or article carried a security classification and, having regard to the circumstances known to the person, it was unjustifiable to take that risk.

27. Why is the term 'proper place of custody' proposed to be defined in regulations, rather than in the Bill? Please provide a copy of the draft regulations and/or an overview of its contents, if any.

The justification for the inclusion of the definition of 'proper place of custody' in the regulations is set out at paragraphs 1349-1352 of the Explanatory Memorandum, extracted below:

> It is necessary to prescribe the meaning of the term proper place of custody in the regulations for the following reasons.
>
> - The definition will involve a level of detail that is not appropriate for inclusion in the Criminal Code. The definition may prescribe proper places of custody for different categories and subcategories of information, such as for information having different security classifications, and for different circumstances, such as where security classified information is being held in a Commonwealth facility, is being transferred between facilities, is being held away from a Commonwealth facility (such as where a person has been approved to work from home, or for event security purposes);
>
> - Prescription in regulations is necessary because of the changing nature of the subject matter. It will be necessary for the definition to keep up to date with changes to Commonwealth protective security policy, to ensure that there is no inconsistency between that which the policy requires or authorises, and that which is subject to the offence provisions;
>
> - The relevant material involves material of such a technical nature that it is not appropriate to deal with it in the Criminal Code. The concept of a proper place of custody for security classified information or information made or obtained by an intelligence agency, for example, may involve technical specifications relating to, for example, the physical, information and personnel security arrangements for that place of custody, and for the accreditation of that place of custody; and
>
> - Elements of the offence may be determined by reference to treaties in order to comply with Australia's international obligations. Australia concludes treaties and international agreements for the handling of certain information, such as classified information received from or given to foreign governments, which may be relevant to the definition of a proper place of custody in relation to such information.
>
> The concept of a proper place of custody should be interpreted broadly for the purposes of determining the matters that may be prescribed in regulations. The proper place of custody for specified information may include, for example:
>
> - a building or part of a building
>
> - a safe, compactus or other place of storage
>
> - a briefcase, bag or other container allowing for the custody of information or documents in transit, or

- an electronic system, computer network, computer or device allowing for the custody of information in electronic form.

The regulations may prescribe that a proper place of custody must meet certain requirements. For example, the regulations may prescribe that a building is only be a proper place of custody for specified information if, and while, it is:

- constructed to meet certain requirements;
- fitted with security systems and measures that meet certain requirements, which are in operation;
- staffed by appropriate security personnel; and
- accredited by an appropriate authority as meeting certain requirements.

A proper place of custody may also include a combination of one or more of the abovementioned places, such as an electronic system that meets certain requirements and that is located in a building or part of a building that meets certain requirements.

Draft regulations have not yet been prepared. The regulations will be prepared consistently with the proposed approach set out in the Explanatory Memorandum, extracted above.

28. *Why is it necessary for there to be regulations setting out code words that may lead to an offence being considered aggravated, rather than setting it out in the text of the Bill? What are these regulations intended to cover?*

The aggravating circumstance in subparagraph 122.3(1)(b)(ii) will apply if the underlying offence involves a record and the record:

- is marked with a code word
- is marked with 'for Australian eyes only'
- is marked as prescribed by the regulations for the purposes of this subparagraph.

In addition to proving that the record carried the relevant marking, the prosecution will need to prove that the person was reckless as to this element. Therefore, in relation to code words, the person will need to have been aware of a substantial risk that the record was marked with a code word and, having regard to the facts and circumstances known to them, it was unjustifiable to take the risk.

A code word will not need to be prescribed in the regulations in order for the aggravating circumstance in subparagraph 122.3(1)(b)(ii) to apply.

As set out in paragraph 1563 of the Explanatory Memorandum:

> A code word is a word or phrase indicating that the information contained in the record is in a special need to know compartment. It is often necessary to take precautions beyond those normally indicated by the security classification to protect particular information. These precautions will be specified by the organisation that owns the information—for instance, those with a need to access

information covered by a code word will typically be given a special briefing about the nature of the information covered by the code word, the reasons for its sensitivity, and the special measures that must be taken to protect it, and required to sign a non-disclosure agreement.

The justification for the regulation-making power to prescribe additional record markings for the purpose of subparagraph 122.3(1)(b)(ii) is set out at paragraph 1565 of the Explanatory Memorandum, extracted below.

> Part 2.3.4 of the Guide to Framing Commonwealth Offences provides that the content of an offence should only be delegated to another instrument where there is a demonstrated need to do so. It is necessary to including a regulation-making power to prescribe additional record markings for the purpose of subparagraph 122.3(1)(b)(ii) because:
>
> - the definition will involve a level of detail that is not appropriate for inclusion in the Criminal Code—there are a variety of record markings, in varying permutations and combinations, that might appropriately be prescribed. For example:
>   - the marking 'AUSTEO' is the standard and commonly used abbreviation of 'for Australian eyes only', and might appropriately be specified in regulations as an alternative marking, and
>   - the marking 'AGAO' (for Australian Government Access Only) is used by the Department of Defence and ASIO to denote that those agencies may pass the marked information to appropriately cleared representatives of foreign governments on exchange or long-term posting or attachment to the Australian Government, but that other agencies are to handle the information as though it were AUSTEO.
> - prescription in regulations is necessary because of the changing nature of the subject matter—it will be necessary for the definition to keep up to date with changes to Commonwealth protective security policy, to ensure that there is no inconsistency between that which the policy requires or authorises, and that which is subject to the offence provisions; and
> - the relevant material involves material of such a technical nature that it is not appropriate to deal with it in the Act—as noted above, there are a variety of protective markings used by the Australian Government, that would appropriately be listed in regulations given their technical nature.

29. *Does this provision allow any code word to be prescribed by the regulations? Or, does the provision only allow code words which have the same meaning and effect as the label 'for Australian eyes only'? If so, can this be made clear in the Bill?*

The application of the provision is described in the answer to Question 28.

Secrecy offences

30. *Does the inclusion of the words 'receiving', 'obtaining', 'collecting' and 'possessing' in the definition of 'deal' mean that a person may have committed an offence simply by being given information that is, for example, security classified? Or, continuing to possess a document, after the recipient becomes aware of its contents?*

The offences at subsections 122.1(2) and 122.2(2) will apply to dealings with inherently harmful information or dealings that cause harm to Australia's interests or will or are likely to cause harm to Australia's interests. The definition of 'deals' covers the terms set out in Question 30.

The fault element of intention will apply to the physical element that a person communicated or otherwise dealt with information.

These offences must be read in combination with the defences in section 122.5, especially subsection 122.5(1) which relates to a person exercising a power, or performing a function or duty, in the person's capacity as a Commonwealth officer.

31. *Would 'deals with' extend to a person intentionally viewing or downloading inherently harmful information that has been unlawfully published on the internet by another person? What about commenting on the content or posting links to it on social media, blogs, threads and other online forums?*

The department thinks it unlikely that simply viewing information would fall within the definition of 'deals'. However, it would depend on the specific facts and circumstances of the case.

The department notes that it is somewhat artificial to consider a situation of 'viewing' alone, as there would likely be other dealings with the information surrounding the viewing which may fall within the relevant definition.

Depending on the facts and circumstances, downloading information may constitute 'possession' of information.

In addition, the department notes that the secrecy offences contain two defences for information already in the public arena.

The first defence (ss 122.5(2)) applies where information has been made public with the authority of the Commonwealth.

The second defence (ss 122.5(8)) applies where a person (who did not make or obtain the information by being a Commonwealth officer) communicates information that has already been communicated by another person and the person reasonably believes that his/her communication will not cause harm to Australia's interests or the security or defence of Australia.

These defences seek to strike a balance between freedom of expression on the one hand, and recognition that further dissemination of harmful information could cause additional harm on the other hand.

32. How does the definition of 'inherently harmful information' comply with the ALRC's recommendations that secrecy offences should target conduct that does, or is reasonably likely to, or is intended to, cause harm to public interests (eg. prejudice national security or endanger life)?

Protecting Australia from espionage and foreign interference relies heavily on having strong protections for information, especially where disclosure causes harm to an essential public interest. The unauthorised disclosure or use of certain information can prejudice national security and defence or our relationships with foreign countries.

Criminal offences are necessary to deter such disclosures and punish them if they do occur.

The key premise of the ALRC's report was that secrecy offences should apply where the disclosure causes harm, is reasonably likely to cause harm or was intended to cause harm to an essential public interest.

The new secrecy offences are consistent with this view, although the Bill implements this in a different way to that envisaged by the ALRC.

The ALRC report is premised on the view that an express harm requirement should be proved. The Bill partially implements this approach in the offence of 'conduct causing harm to Australia's interests' in section 122.2 The ALRC accepted (in Chapter 8 of its report) that the disclosure of some categories of information could be inherently harmful, and that secrecy offences relating to the disclosure of such information would therefore not require an express harm element. This is reflected in the offence at 122.1, which does not require proof of an express harm requirement.

As noted in the department's supplementary submission, the Attorney-General has asked the department to progress changes to the Bill to:

- create separate offences that apply to non-Commonwealth officers that are narrower in scope than those applying to Commonwealth officers and only apply to the most serious and dangerous conduct, and

- improve the clarity of offences that apply to current and former Commonwealth officers, most particularly by narrowing the definitions of 'causes harm to Australia's interests' and 'inherently harmful information' at section 121.1 of the Bill.

33. The term 'inherently harmful information' (section 121.1) includes information that was required to be provided by a person to the Commonwealth in compliance with a legal obligation.

a. What are some examples of the information intended to fall under this part of the definition?

b. Would information about a person's tax return, or mandatory notifications to Centrelink, be classed as 'inherently harmful information'?

The purpose of paragraph (d) of the definition of 'inherently harmful information' is to ensure that information provided to the Commonwealth under a coercive power or other compulsion is

protected. It is considered essential to protect such information where a person has been required to provide it to the Commonwealth, typically under compulsion or penalty for non-compliance. If this information is not adequately protected, it could have the impact of discouraging individuals and companies from providing honest and complete information to the Commonwealth in accordance with an obligation under a law or otherwise by compulsion of law. This harms the ability for Commonwealth authorities to perform their functions.

Paragraphs 1327 and 1328 of the Explanatory Memorandum, extracted below, provide examples of the information intended to fall under paragraph (d):

> Paragraph (d) of the definition provides that information that was provided by a person to the Commonwealth or an authority of the Commonwealth in order to comply with an obligation under a law or otherwise by compulsion of law is a category of inherently harmful information. Paragraph (d) will cover a wide range of information, such as:
>
> - information that is required to be provided to the Australian Taxation Office by taxpayers in accordance with taxation legislation
> - information that is required to be provided to regulatory agencies, such as the Australian Securities and Investments Commission or the Australian Prudential Regulation Authority, under various regulatory regimes
> - information requirement to be provided by carriers and carriage service providers to the Communications Access Co-ordinator, in accordance with telecommunications interception legislation, and
> - information obtained by Commonwealth authorities utilising coercive information gathering powers, including notices-to-produce, production orders, and compulsory questioning.
>
> The unauthorised communication, dealing in, or mishandling of such information has the potential to cause a range of harm to private interests. It is also likely to impact on essential public interests, by discouraging individuals and companies from providing honest and complete information to the Commonwealth in accordance with an obligation under a law, or otherwise by compulsion of law, harming the ability for Commonwealth authorities to perform their functions.

34. *A number of the secrecy offences criminalise communication or dealing with information that would or could 'cause harm to Australia's interests.' For all of these offences, the person need only be reckless as to whether the conduct would or could cause harm to Australia's interests.*

    a. *Given the serious penalties for these offences (5 to 15 years imprisonment) why is there no requirement for a person to know or intend that their conduct will or could cause harm?*

       The department notes that the prosecution will need to prove the physical element that the communication (or other dealing):

       - causes harm to Australia's interests
       - will cause harm to Australia's interests or

- is likely to cause harm to Australia's interests.

In addition to proving this physical element, the prosecution will also have to prove that the defendant was reckless as to this element. That is, the defendant will need to have been aware of a substantial risk that his or her conduct would cause harm to Australia's interests (for example) and, having regard to the facts and circumstances known to him or her, it was unjustifiable to take the risk.

The default fault element for a result element is recklessness (see subsection 5.6(2) of the Criminal Code) so this offence is consistent with the principles of criminal responsibility set out in Chapter 2 of the Criminal Code. This is still a high bar for the prosecution.

The application of the fault elements of intention or knowledge to this element of the offence would make it more difficult to prove. It is less likely that the Commonwealth could prove these fault elements beyond a reasonable doubt in the context of this element.

Commonwealth criminal law policy, as set out in the *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*, is that each offence should have a single maximum penalty that is adequate to deter or punish a worst case offence, including repeat offences. The maximum penalty should aim to provide an effective deterrent to the commission of the offence, and should reflect the seriousness of the offence within the relevant legislative scheme.

The maximum penalties for each of the offences in the Bill appropriately reflect the 'worst case scenario' for that offence. A sentencing court will clearly have the discretion to set the penalty at an appropriate level to reflect the relative seriousness of the offence based on the facts and circumstances of the particular case.

35. *The secrecy offences will only apply where the information was made or obtained by a Commonwealth officer or person performing work for a Commonwealth entity. The person need only be reckless as to whether the information was so made or obtained.*

    a. *Given the serious penalties for these offences (5 to 15 years imprisonment) why is there no requirement for a person to know that the information they are communicating or dealing with was made or obtained by a Commonwealth officer.*

The default fault element for a circumstance element is recklessness (see subsection 5.6(2) of the Criminal Code) so this element of the offence is consistent with the principles of criminal responsibility set out in Chapter 2 of the Criminal Code. This is still a high bar for the prosecution.

The application of the fault elements of knowledge to this element of the offence would require the prosecution to prove that the person is aware that it exists or will exist in the ordinary course of events. Recklessness requires proof that the person was aware of a substantial risk that the circumstance exists or exists and, having regard to the circumstances known to him or her, it is unjustifiable to take the risk (see sections 5.3 and 5.4 of the Criminal Code).

Applying the fault element of knowledge to this element will make the offence more difficult to prove. It is less likely that the Commonwealth could prove this fault element beyond a reasonable doubt.

36. *The Bill criminalises the handling of Commonwealth information in a way that 'causes harm to Australia's interests'. which are defined to include Australia's international relations, including economic relations.*

    a. *Could a person be culpable in relation to this offence if they communicated information that exposed flaws in a trade agreement between Australian and another country?*

    b. *Is it appropriate that such information be treated in the same way as information that harmed Australia's defence or intelligence capabilities*

    Scenario: An advocacy group received unclassified information from a former government employee that raises concerns about a particular trade agreement being negotiated between Australia and another country. The advocacy group uses the information to inform its ongoing campaign against the agreement, including a series of online articles. Would this conduct be captured in any of the espionage or secrecy offences? If so, is a defence available?

In this situation, section 122.2 would require the Commonwealth to prove, beyond a reasonable doubt, that the communication of the information:

- caused harm to Australia's interests
- will cause harm to Australia's interests or
- is likely to cause harm to Australia's interests.

Consistent with the definition of 'causes harm to Australia's interests', the prosecution would have to prove that the communication did, would or was likely to harm or prejudice Australia's international relations, as defined in the Bill. This would require proof that the communication did, would or was likely to harm or prejudice Australia's political, military and economic relations with foreign governments and international organisations

In addition to proving these matters, the prosecution would have to prove, beyond a reasonable doubt, that the person was reckless as to this element. That is, the defendant will need to have been aware of a substantial risk that his or her conduct would cause this harm to Australia's interests and, having regard to the facts and circumstances known to him or her, it was unjustifiable to take the risk.

It is not possible to provide a definitive answer on whether a communication that 'exposed flaws in a trade agreement' would meet these elements, as it will depend on all of the facts and circumstances of the case. However, the scenario set out at Question 36 does not identify any harm or likely harm.

In relation to the espionage offences, the person will have to deal with information in a way that makes it available to a foreign principal. The person must also intend to, or be reckless as to whether his or her conduct would, prejudice Australia's national security.

37. *Would Commonwealth employees and affiliates dealing with security classified information (ie. 'inherently harmful information') as part of their job satisfy the elements of an offence (disregarding any defence)?*

    a. *If yes, why should the everyday activities of Commonwealth employees and affiliates that involve dealing with, or communicating, 'inherently harmful information' rely on a statutory defence to the secrecy offences? Why isn't it an element of the offence that the conduct is outside the officer's duties?*

    Scenario: An Australian Government employee intentionally obtains, produces, retains, copies and communicates a range of classified documents as part of her everyday duties. In doing so, she has met all the requirements for the aggravated offences in relation to communicating and dealing with inherently harmful information.

See answer to Question 23.

38. *To be lawful under the proposed secrecy provisions, foreign partners will need to rely on the statutory defence for dealing with information in accordance with an agreement with the Commonwealth (section 122.5(1)(b)) in order to share information with Australian intelligence and law enforcement agencies.*

    a. *Does framing the secrecy offences and defences in this way risk hampering co-operation with our foreign partners?*

    Scenario: Foreign government law enforcement allies request a criminal check on an Australian citizen from an Australian agency. Could this conduct be captured by the elements of the offence, and if so, would the officer have to rely upon a defence?

    Scenario: An Australian intelligence agency provides their five-eyes partners with access to a number of intelligence reports. One of the partner agencies uses the intelligence for the purpose of internal briefings to senior staff; as context in a number of closely-held internal documents; and as the basis of an alert placed on the country's migration system. Could this conduct be captured by the elements of the offence, and if so, would the officers have to rely upon a defence?

Agencies have been consulted about the application of the offences in this context.

39. *To what extent are members of parliament, ministers and their staff covered by the defence in section 122.5(1)?*

Members of parliament, ministers and their staff are covered by the definition of 'Commonwealth officer' in section 121.1 of the Bill and therefore covered by the defence in subsection 122.5(1). Paragraph 1304 of the Explanatory Memorandum is extracted below.

Paragraph (b) of the definition provides that a Commonwealth officer includes an individual appointed or employed by the Commonwealth otherwise than under the *Public Service Act 1999*. This includes, but is not limited to:

- a Minister of State (including a Parliamentary Secretary) appointed by the Governor-General in Council under section 64 of the Constitution
- statutory officers, such as the Director-General of Security appointed by the Governor-General under section 7 of the *Australian Security Intelligence Organisation Act 1979*
- an individual employed under the *Members of Parliament (Staff) Act 1984*, or
- an individual employed under the *Parliamentary Service Act 1999*.

40. Could a member of parliament who handled classified information as part of their parliamentary duties (for example, a member of this Committee) be considered to have dealt with 'inherently harmful information'?

Scenario: a member of parliament receives sensitive information from a whistle-blower in relation to a recent operation by a law enforcement agency.

Scenario: a minister's staff member receives a classified briefing from a government department.

Scenario: members of the PJCIS receives classified information from an intelligence agency during an inquiry.

Yes, a member of parliament may 'deal' with inherently harmful information. However, the department notes that the offences should not be read without also considering the available defences, including subsection 122.5(1). The defences are an integral part of the overall offence framework and the offences cannot be properly construed if the defences are not taken into account.

The department notes that members of the PJCIS are already subject to specific offences in Schedule 1 of the *Intelligence Services Act 2001* and Part V of the ASIO Act.

41. What is the term 'fair an accurate reporting' intended to include, and not include, in relation to the proposed defence for journalists? Why was this wording selected?

Paragraph 1640 of the Explanatory Memorandum is extracted below.

However, a person will only have the benefit of the defence in their capacity as a journalist 'engaged in fair and accurate reporting'. The concept of being engaged in fair and accurate reporting is used within section 18D of the Racial Discrimination Act 1975. In this context, it is intended that the requirement for the journalist to be engaged in fair and accurate reporting will limit the scope of the defence to journalists who are, in fact, engaged in such reporting, excluding persons who:

- merely publish documents or information without engaging in fair and accurate reporting
- use information or documents to produce false or distorted reporting, or

- are not, in fact, journalists engaged in fair and accurate reporting—for example, where the person is an officer or agent of a foreign intelligence service engaged in a foreign interference effort.

As noted in the department's supplementary submission, the Attorney-General has asked the department to progress changes to the Bill to strengthen the defence for journalists (at subsection 122.5(6)) by removing any requirement for journalists to demonstrate that their reporting was 'fair and accurate', ensuring that the defence is available where a journalist reasonably believes that their conduct was in the public interest, and clarifying that the defence is available for editorial and support staff as well as journalists themselves.

42. Who determines whether something is 'fair and accurate?' Is it a subjective test, based upon the information available to the journalist before reporting; an objective test; or a combination of the two?

As noted in the department's supplementary submission, the Attorney-General has asked the department to progress changes to the Bill to strengthen the defence for journalists (at subsection 122.5(6)) by removing any requirement for journalists to demonstrate that their reporting was 'fair and accurate', ensuring that the defence is available where a journalist reasonably believes that their conduct was in the public interest, and clarifying that the defence is available for editorial and support staff as well as journalists themselves.

43. What is the term 'public interest' intended to include, and not include, in relation to the proposed defence for journalists?

Paragraphs 1641 of the Explanatory Memorandum is extracted below.

> The defence will also only be available where the person's conduct is in the public interest. It will ordinarily be a matter for the person to adduce or point to evidence that suggests a reasonable possibility that their conduct was in the public interest, by reason of section 13.3 of the Criminal Code. It will ordinarily then be a matter for the prosecution to disprove the defence beyond reasonable doubt. However, subsection 122.5(7) provides that, without limiting paragraph (6)(a), dealing with or holding certain information will not be in the public interest, being:
>
> - information protected by section 92 of the ASIO Act—which protects the identity of ASIO employees and ASIO affiliates
> - information protected by section 41 of the *Intelligence Services Act 2001*—which protects the identity of the staff and agents of the Australian Secret Intelligence Service
> - dealing with or holding information that would be an offence under section 22, 22A or 22B of the *Witness Protection Act 1994* – which protects the identity of Commonwealth, Territory, State participants or information about the National Witness Protection Program, and
> - information that will or is likely to harm or prejudice the health or safety of the public or a section of the public.

The Bill does not seek to define public interest beyond the exclusions listed in subsection 122.5(7). This allows the defendant to adduce or point to evidence that suggests a reasonable possibility that

the person held or dealt with the information in the public interest (as required in order to discharge an evidential burden consistent with subsection 13.3(6) of the Criminal Code). Once this burden is discharged, the prosecution will then be required to prove the person did not hold or deal with the information in the public interest beyond reasonable doubt.

As noted in the department's supplementary submission, the Attorney-General has asked the department to progress changes to the Bill to strengthen the defence for journalists (at subsection 122.5(6)) by removing any requirement for journalists to demonstrate that their reporting was 'fair and accurate', ensuring that the defence is available where a journalist reasonably believes that their conduct was in the public interest, and clarifying that the defence is available for editorial and support staff as well as journalists themselves.

44. Does the proposed defence for journalists extend to persons assisting in the publication of a story? For example, printing and publishing staff, administrative assistants, legal advisors or editors.

The defence is limited to journalists. This term is not defined and will take its ordinary meaning.

As noted in the department's supplementary submission, the Attorney-General has asked the department to progress changes to the Bill to strengthen the defence for journalists (at subsection 122.5(6)) by removing any requirement for journalists to demonstrate that their reporting was 'fair and accurate', ensuring that the defence is available where a journalist reasonably believes that their conduct was in the public interest, and clarifying that the defence is available for editorial and support staff as well as journalists themselves.

45. Why is there a 'public interest' defence available to journalists, but no such defence available for a whistle-blower who is a journalist's source?

There are established mechanisms for Commonwealth officers to make public interest disclosures under the Public Interest Disclosure Act. The inclusion of a general public interest defence would disrupt the primacy of the Public Interest Disclosure Scheme as the mechanism for making disclosures of information.

The defence in subsection 122.5(4) could be broadened to cover other Commonwealth public interest disclosure schemes. The department notes however that neither it nor submissions have identified circumstances in which whistleblowers under other schemes would be dealing with inherently harmful information or information that causes harm to Australia's interests.

46. Why do the defences in section 122.5 only extend to the secrecy offences relating to communication of information to the IGIS, the Ombudsman, ACLEI, a court or tribunal or in accordance with the PID Act?

a. Why are the offences of dealing with or removing from a proper place of custody not covered by these defences (for example a person has 'dealt with' the information intended to communicate it to the IGIS, but has not yet done so)?

Scenario: An employee of a government agency has concerns about maladministration within their organisation and wants to report the matter to the Ombudsman for investigation. The employee copies some 'protected' level documents from the agency's records management system and emails them over a protected network to the Ombudsman's office. The defence in subsection 122.5(3) applies to the employee's communication of the information, but does not appear to apply in relation to their copying and removal of the information.

The defences at subsections 122.5(3) and (5) do not explicitly extend to conduct involving dealings with information other than communications. The defences could be explicitly extended to cover a broader range of dealings.

The department notes that, in relation to security classified information, there are significant risks attached to inappropriate storage or handling of such information. An extended defence would have the effect of not criminalising improper handling of highly classified information, leaving conduct that may be preparatory to more serious offences un-addressed.

47. Why does the defence in proposed section 122.5(8) only apply to communication of previously published information, and not dealing with such information?

Scenario: A member of the public downloads a copy of a leaked classified document that has been published on the WikiLeaks website and saves it to their computer. The person then emails a copy of the document to some friends. The defence in section 122.5(8) applies to the sending of the email; however, there appears to be no defence for the act of downloading the document to their computer. Does the behaviour engage the elements of a secrecy offence?

The defence at subsection 122.5(8) does not explicitly extends to conduct involving dealings with information other than communications. The defence could be explicitly extended to cover a broader range of dealings.

The department notes that, in relation to security classified information, there are significant risks attached to inappropriate storage or handling of such information.

48. There is currently no specific defence in the Bill enabling information to be dealt with for the purpose of seeking legal advice. Is the defence to communication offences set out in s. 122.5(9) intended to allow this? The Committee notes the limited scope of this defence. Would there be any potential impediments to a specific defence being added?

It is not the intention of the offences to cover situations where a person is seeking legal advice about their ability to communicate information, or the application of the offences. A specific defence could provide clarity in relation to such activities.

49. Why is the Attorney-General's consent not proposed to be required for a prosecution under the secrecy offences, in contrast to the existing laws and the other offences in the Bill? Could this be considered?

The Attorney-General's consent is commonly required to commence proceedings that could affect Australia's international relations or national security. These are considerations that the Commonwealth Director of Public Prosecutions is not able to take into account under the Prosecution Policy of the Commonwealth.

Such provisions provide the Attorney-General with an opportunity to receive advice from relevant agencies and other Ministers on sensitivities that might arise if proceedings are commenced for offences, and provides opportunity for consideration of whether the prosecution could be detrimental to Australia's foreign relations and national security.

Secrecy offences do not inherently raise such considerations.

Espionage offences

50. What type of information would 'concern' Australia's national security? Could this include private citizen's view on Australia's trade, military or political relations?

Although it is not possible to give a definitive answer about a hypothetical scenario, the department does not consider it likely that a private citizen's view or opinions on Australia's trade, military or political relations would be information that 'concerns Australia's national security'.

In this regard, the Bill is consistent with the drafting of existing subparagraph 91.1(1)(a)(i) of the Criminal Code, which refers to information 'concerning the Commonwealth's security or defence'. The department is not aware of this phrase being tested.

51. Given that the proposed espionage offences do not require the information to originate from government, could these espionage offences cover privately, professionally or commercially produced research, opinions, advice or analysis made available to foreign principals?

Yes, the offences could cover such material. In particular, section 91.2 applies to any information and does not require it to be security classified or concern national security.

The department notes that existing espionage offences are not limited to information originating from government.

52. Could the proposed espionage offence capture private discussions a person has with a foreign contact? For example, where a private citizen proffers an opinion which is critical of government decision making or conduct?

The espionage offences in sections 91.1 and 91.2 of the Bill require the prosecution to prove, amongst other things, that:

- the person's conduct resulted or would result in the information being made available to a foreign principal or a person acting on behalf of a foreign principal
- the person was reckless as to whether his or her conduct would have this result, and
- that the person intended to (or was reckless as to whether his or her conduct would) prejudice Australia's national security or, if the information is security classified or concerns national security, to advantage the national security of a foreign country.

It is not possible to provide a definitive answer on whether a 'private conversation' with a 'foreign contact' would meet these elements, as it will depend on all of the facts and circumstances of the case.

53. Has AGD consulted with universities or considered what impact the espionage provisions could have on universities?

The department has not consulted universities. The department considered a range of scenarios in formulating the draft offences.

a. Can information produced by universities 'concern Australia's national security' (within the meaning of ss 91.1 and 91.3)? If so, what impact will this have on international partnerships, secondments, research or conferences?

Information produced by universities could potentially be information 'concerning Australia's national security'. However, the department notes the answer to Question 52 about the elements that will need to be proved in relation to espionage offences.

b. If a university provides course content with a nexus to national security (i.e Australia's economic relations), and the cohort includes international students with a connection to a foreign principal (a foreign government, foreign-owned enterprises or a foreign organisations such as the UN) has the university made the information available, within the meaning of sections 91.1(2) or 91.3?

It is not possible to provide a definitive answer, as it will depend on all of the facts and circumstances of the case. However, in the absence of any special circumstances or particular link to a foreign government , an international student is unlikely to be considered to be a foreign principal or a person acting on behalf of a foreign principal for the purposes of the espionage offences.

c. Can university conduct be captured by s. 91.2(2)?

Any person's conduct could be captured by subsection 91.2(2).

54. For the purpose of the espionage offences, does online publication 'make available' information? (for example, an online newspaper, a blog-post, a tweet, an online academic journal, or the websites of public interest groups, charities and the like)

A person can deal with information by publishing it online. However, the department notes the answer to Question 52 about the elements that will need to be proved in relation to espionage offences.

55. If 'make available' is not intended to include publication (online or otherwise), why not? Would this not defeat the purpose of the provision? For example, a person could not directly provide information to a foreign intelligence agency, but they could publish it online, where it could come to the attention of the intelligence agencies of multiple countries.

The definition of 'deals' in section 90.1 specifically covers both 'making available' (paragraph (j)) and 'publishing' (paragraph (i)).

56. Would there be any practical difficulties with defining 'make available' in the Bill (in addition to the current definition in relation to material)?

Paragraph 544 of the Explanatory Memorandum explains the term 'makes available' for the purpose of the definition of 'deals' in section 90.1. The relevant section of the paragraph is extracted below. It is not considered necessary to provide further definition of this term in the Bill itself.

> *Makes it available* is intended to cover the passage of information or articles other than by disclosing or publishing it. This is intended to cover situations where arrangements are made between two individuals to pass information using a pre-arranged location, without the individuals needing to meet. For example, Person A may leave a classified document in a particular letterbox and Person B (who is acting on behalf of a foreign principal) will later come and collect it. Another example would be where Person A gives the document to Person C, who will then pass it on to Person B (who is acting on behalf of a foreign principal). Although it is arguable that Person A has 'communicated' the document in these situations, it is intended that the term 'makes it available' will provide clarity in situations where intermediaries are used.

57. Would the United Nations, the World Trade Organisation, and North Atlantic Treaty Organisation be considered 'foreign principals' for the purpose of the Bill?

Paragraph 562 of the Explanatory Memorandum, extracted below, explains the meaning of the term 'public international organisation' in paragraph 90.2(b).

> The term will include multi-lateral international organisations such as the World Bank, the World Trade Organisation and the International Monetary Fund. In some situations, the provision of information to such organisations could prejudice Australia's national security and constitute espionage. For example, Person I is an official of International Organisation Z and obtains confidential information concerning a significant impending change in Australia's economic policies from Person J, an Australian official who intends to harm Australian interests for ideological reasons. International

Organisation Z uses this information to undermine Australia's position in multilateral trade negotiations, causing significant damage to Australia's international relationships.

58. *Would Australian companies working with foreign public enterprises be captured by the offences? For example, by providing professional advice.*

The department notes the answer to Question 52 about the elements that will need to be proved in relation to espionage offences.

It is not possible to provide a definitive answer on whether the provision of professional advice to a foreign public enterprise would meet these elements, as it will depend on all of the facts and circumstances of the case.

59. *Does the inclusion of terrorist organisations reflect a gap in current offence provisions?*

    a. *Does the inclusion of terrorist organisations extend the concept of espionage (making, in effect, a range of terrorist activities a subset of espionage)?*

The inclusion of terrorist organisations in the definition of 'foreign principal' is intended to ensure that there are no gaps in relation to such organisations, given the significant consequences for Australia's security should an offence against Part 5.2 be committed by a person acting on behalf of a terrorist organisation.

The inclusion does not make terrorist activities a 'subset' of espionage. It ensures that the passage of information to a terrorist organisation with an intention to prejudice Australia's national security (or advantage the national security of a foreign country, in some circumstances) falls within the scope of espionage offences and is matched by appropriately serious penalties.

60. *Would comments made by industry lobby groups, universities and media organisations in the course of their regular activities be capable of meeting the threshold of recklessness as to whether conduct will prejudice Australia's national security or advantage the national security of a foreign country (s. 91.1(2))?*

The department notes the answer to Question 52 about the elements that will need to be proved in relation to espionage offences.

The application of recklessness as a fault element will mean that the prosecution will have to prove, beyond a reasonable doubt, that the person was aware of a substantial risk that his or her conduct would prejudice Australia's national security or advantage the national security of a foreign country and, having regard to the facts and circumstances known to the person, it was unjustifiable to take the risk.

It is not possible to provide a definitive answer on whether the regular activities of lobby groups, universities and media organisations would meet the elements of an espionage offence, as it will depend on all of the facts and circumstances of the case. However, the usual bona fide activities of universities and academics are not expected or intended to fall within the scope of the offences, given that they will not be undertaken with an intention to, or reckless as to whether they will, prejudice Australia's national security or advantage the security of a foreign principal.

61. *Why is the fact that information contains code word material an aggravating factor for the secrecy offences, but not the espionage offences?*

The different aggravating circumstances for espionage and secrecy offences reflect the differences between the offences. Information being marked with a code word could also be listed as an aggravating circumstance for the aggravated espionage offence at section 91.6.

62. *Unlike the other espionage offences, s. 91.3 does not require the person to intend any outcome, or be reckless to it (whether it be prejudice to Australia's national security, or advantaging another country's national security).*

    a. *Was this deliberate?*

    Yes.

    b. *Is a penalty of 20 years imprisonment appropriate where a person does not actually intend to cause harm?*

    Yes. Commonwealth criminal law policy, as set out in the *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*, is that each offence should have a single maximum penalty that is adequate to deter or punish a worst case offence, including repeat offences. The maximum penalty should aim to provide an effective deterrent to the commission of the offence, and should reflect the seriousness of the offence within the relevant legislative scheme.

    As set out at paragraph 706 of the Explanatory Memorandum, the worst case scenario for the offence at section 91.3 is the communication of highly classified information to a foreign country. This is exceptionally harmful conduct, regardless of whether the person intended to prejudice Australia's national security or advantage the national security of a foreign country.

    A sentencing court has the discretion to set the penalty at an appropriate level to reflect the relative seriousness of the facts and circumstances of the particular case.

63. *Why is the 'prior publication' defence is s 122.5 not also available for espionage offences?*

This defence is not considered appropriate. For sections 91.1 and 91.2, the offence includes the element that the person intended to, or was reckless as to whether his or her conduct would, prejudice Australia's national security (or advantage the national security of a foreign country).

64. *What defences are available to persons who are not engaged with the Commonwealth, for example:*

    a. *Academics and universities;*

    b. *Media organisations;*

    c. *Public interest groups;*

d. Lobby groups and associations;

e. Lawyers and other advisors;

f. International organisations; and

g. Private citizens

Sections 91.4, 91.9 and 91.13 provide defences where a person dealt with information or an article in accordance with a law of the Commonwealth or in accordance with an arrangement or agreement to which the Commonwealth is party and which allows for the exchange of information or articles.

Sections 91.4 and 91.9 also provide defences where a person deals with information that has already been communicated or made available to the public with the authority of the Commonwealth.

The general defences in Part 2.3 of the Criminal Code will also apply, including the defence of lawful authority at section 10.5.

65. Could a public interest group uncovering serious government corruption on their website be caught by the proposed offences? For example, would the conduct of organisations like WikiLeaks and the International Consortium of Investigative Journalists (which published the Panama Papers) be captured by espionage offences?

The espionage offences in sections 91.1 and 91.2 of the Bill require the prosecution to prove, amongst other things, that:

- the person's conduct resulted or would result in the information being made available to a foreign principal or a person acting on behalf of a foreign principal
- the person was reckless as to whether his or her conduct would have this result, and
- that the person intended to (or was reckless as to whether his or her conduct would) prejudice Australia's national security or, if the information is security classified or concerns national security, to advantage the nationals security of a foreign country.

It is not possible to provide a definitive answer on whether the conduct described in Question 65 would meet these elements, as it will depend on all of the facts and circumstances of the case.

a. Is there, or should there be, a public interest defence?

It is hard to see how the passage of classified information or information relevant to national security to a foreign principal could be in the public interest, where it is done with an intention to prejudice Australia's national security or advantage the national security of a foreign country.

Similarly, it is difficult to see how the passage of unclassified information to a foreign principal, with an intention to prejudice Australia's national security, would be in the public interest.

There are established mechanisms for Commonwealth officers to make public interest disclosures under the Public Interest Disclosure Act.

66. *What conduct engaged in by private citizens, academics and journalists, if any, would fall within s. 91.4(1)(a), but not the general defence at s 10.5?*

The department is not able to speculate on what conduct would fall within the defence at section 91.4(1)(a) but not the general defence at section 10.5 of the Criminal Code. The department's view is that the reference to conduct being 'in accordance with' a law of the Commonwealth may be broader than the requirement in section 10.5 for the conduct to be 'justified or excused' by a law of the Commonwealth.

67. *Could the conduct of our allies, acting outside of Australia, be captured by the espionage offences? If so, would Australia's allies be required to rely on a statutory defence in order to request or receive information from Australia? Could this hamper Australia's relations with its allies and partner agencies? Were Australian agencies consulted about this?*

Australia's Five Eyes allies are unlikely to be engaged in espionage activities against Australia.

Australian agencies were consulted about this.

68. *How do the proposed espionage and secrecy offences engage with:*

    a. *the implied right to freedom of political communication; and*

    The department considered the implied freedom of communication and is confident that the offences in the Bill do not infringe the implied freedom.

    b. *the right to freedom of expression in Article 19 of the International Covenant on Civil and Political Rights?*

    To the extent that the Bill promotes this right, this is addressed in paragraphs 25-33 of the Explanatory Memorandum.

    To the extent that the Bill limits this right, this is addressed in paragraphs 96-106 of the Explanatory Memorandum.

69. *Please consider the following hypothetical scenario:*

A Commonwealth officer leaks documents to a journalist. The documents contain material from a number of 'secret' reports. The following occurs:

- *An administration officer works for a major paper. The editor directs the officer to copy a number of documents for the journalist.*
- *The newspaper publishes the journalist's article, based on the leaked documents. A number of foreign government embassies have subscriptions.*
- *The newspaper article is published online. The paper has a number of foreign subscribers.*

- *An academic prints a copy of the article, which he keeps in his office.*
- *The academic gives a copy of the article to a colleague. Following detailed discussions they co-author an academic paper on the topic, quoting parts of the report. The academics are aware the paper may prejudice Australia's international relations, but consider the publication of the paper to be in the public interest.*
- *An academic journal publishes the paper. The journal has a number of foreign subscribers, including universities and organisations (i.e. the World Trade Organisation).*

To what extent would the conduct in this scenario satisfy the elements of any of the espionage or secrecy offences?

In particular:

a. *By publishing the information has it been 'made available' to a foreign principal for the purposes of Division 91 (espionage)?*

b. *What defence(s), if any, do the journalist and newspaper have available to espionage? If none, what is the utility of the 'fair and accurate reporting' defence in Division 122 (secrecy)?*

c. *What defence(s), if any, do the academics and journal have available to espionage and secrecy (both dealings and communication)? It appears that s. 122.5(8) would not apply.*

d. *Would the whistle-blower have a defence?*

The department is not able to provide a definitive answer in relation to this scenario as each case will depend on its facts and circumstances, as well as the admissible evidence. The department notes that any analysis of a hypothetical should refer back to all of the elements of the offence as well as considering available defences.

Foreign interference offences

70. *The proposed new foreign interference offences involving a foreign intelligence agency (Subdivision C) are similar to the terrorist organisation offences in Division 102 of the Criminal Code. Why was the structure of the terrorist organisation offences not adopted here (e.g. s. 102.7)?*

The structure of the terrorist organisation offences in sections 102.6 and 102.7 was used as a relevant model for the offences.

71. *For the foreign interference offences involving a foreign intelligence agency, what fault element applies in relation to support, resources or funding being provided to or on behalf of 'a person acting on behalf of an organisation?'*

The fault element of intention will apply to this element. The definition of intention is set out at section 5.2 of the Criminal Code.

72. *What does the person providing the support need to know about the person they provide the information to? Do they need to*

    - *know that the person they provide the support to acts on behalf of an organisation, or*
    - *be reckless as to whether that person acts on behalf an organisation?*

The person will have to intend to provide support or resources to an organisation or a person acting on behalf of the organisation. The definition of intention is set out at section 5.2 of the Criminal Code.

73. *For the foreign interference offences involving a targeted person, a person need only be reckless as to whether their activities are on behalf of a foreign principal, but they must then intentionally conceal or fail to disclose to the targeted person the fact that the activities are on behalf of a foreign principal. How can a person be reckless about whether something is on behalf of a foreign principal, but then intentionally conceal that circumstance from another?*

The fault element of intention applies to paragraphs 92.2(2)(d) and 92.3(2)(d) because the act of concealing something is conduct and therefore must be done intentionally. The department does not see a conflict between the elements described in Question 73.

Interaction with Foreign Influence Transparency Scheme

74. *Are the foreign interference offences intended to overlap with conduct that is regulated by the Foreign Influence Transparency Scheme? If yes, how are they intended to interact?*

The offences are not intended to overlap. The department's view is that they complement each other as described in the department's evidence to the Committee. .

75. *Could the fact a person is registered under the Foreign Influence Transparency Scheme be used to prove an element of one of the foreign interference offences?*

Registration under the Foreign Influence Transparency Scheme could indicate that a person is engaged in registrable activities for the purpose of influencing a political or governmental process. This may be relevant for paragraphs 92.2(1)(c)) and 92.3(1)(c).

76. *Could the fact a person is registered under the Foreign Influence Transparency Scheme be used as a defence to a prosecution of a foreign interference offence, namely that public registration means a person's conduct cannot be 'covert'?*

Section 92.5 sets out the specific defences for the foreign interference offences in the Bill. These defences will apply where the person engaged in the conduct:

- in accordance with a law of the Commonwealth
- in accordance with an arrangement or agreement to which the Commonwealth is party, or
- in the person's capacity as a public official.

Registration of activities will not necessarily mean activities are not covert – noting that a registrant would be unlikely to register in a manner that discloses the commission of an offence.

Other matters

77. Why has a preparatory foreign interference been included, rather than relying on existing provisions in the Criminal Code regarding conspiracy and attempt?

Preparatory offences in Commonwealth legislation are generally reserved for serious criminal conduct warranting criminalisation at the preparation stage.

This offence will give law enforcement authorities the means to deal with preparatory conduct, without the need to, for example, wait until a foreign interference offence is committed or an Australian process is put at risk of interference.

Liability for attempt arises from conduct that is 'more than merely preparatory' (subsection 11.1(2) of the Criminal Code). The proposed offence targets conduct that occurs before liability for attempt would arise. Conduct that amounted to an attempt to commit a foreign interference offence would not capture the range of conduct that the proposed offence would cover.

An offence of attempt carries the same penalty as the primary offence. In recognition of the nature of the preparatory offence, it carries a lower penalty than that applying to the primary foreign interference offences.

78. Will the foreign interference offences apply where the foreign principal engages in the conduct directly? (ie. no need for another person to engage in the conduct 'on behalf of the foreign principal'). If no, in what circumstances would the foreign principal's role in funding or directing the offending by the other person be a criminal offence?

The foreign interference offences will apply where:

- the person is engaging in the conduct on behalf of, or in collaboration with, a foreign principal
- the person is engaging in the conduct on behalf of, or in collaboration with, a person acting on behalf of a foreign principal
- the conduct is directed, funded or supervised by a foreign principal, or
- the conduct is directed, funded or supervised by a person acting on behalf of foreign principal.

79. The Bill provides that category B geographical jurisdiction will apply to the foreign interference offences (at sections 92.2 to 92.4); however no reference is made to the geographic jurisdiction for the foreign interference offences involving foreign intelligence agencies (sections 92.7 to 92.10).

a. Is standard geographic jurisdiction intended to apply to the foreign interference offences involving a foreign intelligence agency?

Yes. Standard geographical jurisdiction will apply to these foreign interference offences.

b. If yes, why is standard appropriate for these foreign interferences but not others?

The conduct targeted by the offences in Subdivision C is different to that targeted by the offences in Subdivision B. The offences in Subdivision B appropriate carry extended geographical jurisdiction to ensure that Australia's political and governmental processes are protected from foreign interference, regardless of there the conduct occurs.

The conduct targeted by the offences in Subdivision C seek to prevent support being given to foreign intelligence services by Australians or from within Australia. This is not considered to be a situation where Australia's criminal law should extend beyond standard geographical jurisdiction. If a person provides support to a foreign intelligence service in another country then, based on the elements of the offences in Subdivision C, it is not immediately apparent that there is a link to Australia that should be punished under Australian criminal law.

80. The foreign interference offences require the person to <u>intend</u> to influence a process or achieve an outcome (ie. influence a political process or prejudice Australia's national security).

- *Is the intention of the foreign principal relevant?*
- *If yes, how?*
- *If no, why not?*

The offences in Subdivision B of Division 92 apply where a person *intends* to influence a process or achieve a particular outcome (paragraph 92.2(1)(c)) or where a person is *reckless* as to whether his or her conduct will influence a process or achieve a particular outcome (paragraph 92.3(1)(c)).

The offences also require (paragraphs 92.2(1)(b) 92.3(1)(b)) that:

- the person is engaging in the conduct on behalf of, or in collaboration with, a foreign principal
- the person is engaging in the conduct on behalf of, or in collaboration with, a person acting on behalf of a foreign principal
- the conduct is directed, funded or supervised by a foreign principal, or
- the conduct is directed, funded or supervised by a person acting on behalf of foreign principal.

The person must also be reckless as to this element.

The connection between the person's conduct and the foreign principal will need to be proved in the context of the elements of the offence at paragraphs 92.2(1)(b) 92.3(1)(b).

81. *Unlike the other foreign interference offences, the foreign interference offences involving a foreign intelligence agency (Subdivision C) do not require the person to intend any outcome (whether it be harm to Australia's national security, or advantaging the foreign intelligence agency).*

    - *Was this deliberate?*

    Yes.

    - *Is a penalty of 15 years imprisonment appropriate where a person does not actually intend to cause harm?*

    The penalty for the offence at section 92.7 is justified at paragraph 1069 of the Explanatory Memorandum, which is extracted below.

> The maximum penalty of 15 years imprisonment is appropriate when compared with the maximum penalty for the offence of providing support to a terrorist organisation in section 102.7 of the Criminal Code, which carries a penalty of 25 years imprisonment. This higher penalty applying to section 102.7 reflects the higher risk to the life of members of the public associated with supporting a terrorist organisation. A penalty of 15 years for this offence is appropriate to recognise the serious harm that can be caused to Australia's sovereignty, national security and other interests as a result of foreign intelligence organisations undertaking operations in, or against, Australia.

Sabotage offences

82. *Why does the proposed definition of 'public infrastructure' include private infrastructure? Should the sabotage offences relating to private infrastructure be separate offences?*

The Explanatory Memorandum explains the need to cover privately owned infrastructure in the definition of public infrastructure at paragraph 230, extracted below.

> It is essential to cover privately owned infrastructure within the definition of ***public infrastructure*** because the consequences flowing from damage to these types of infrastructure could be as damaging as damage to infrastructure owned by the Commonwealth.

Private infrastructure is only being included to the extent that the Commonwealth has constitutional power to legislate.

The department does not consider that there is a justification for covering private infrastructure in separate offences. The department considers that sabotage in relation to private infrastructure can be equally damaging to Australia's interests as sabotage in relation to infrastructure owned by the Commonwealth and therefore should carry the same maximum penalty.

83. *Could a person carrying out dangerous and difficult repairs to a large piece of infrastructure be considered to be reckless?*

The definition of recklessness at section 5.4 requires a person to be aware of a substantial risk that the result will occur and, having regard to the circumstances known to him or her, it is unjustifiable

to take that risk. In the context of essential repairs to public infrastructure, the risk is likely to be justified.

The elements of the sabotage offences also require a person to have intended to, or be reckless as to whether his or her conduct would, prejudice Australia's national security or advantage the national security of a foreign country.

84. Could everyday benign use of public infrastructure that results in damage result in a prosecution under this Bill?

'Everyday benign' use of public infrastructure is highly unlikely to fall within the sabotage offences.

The sabotage offences require the prosecution to prove that a person was reckless as to whether his or her conduct would damage public infrastructure. This requires a person to be aware of a substantial risk that the result will occur and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk.

The elements of the sabotage offences also require a person to have intended to, or be reckless as to whether his or her conduct would, prejudice Australia's national security or advantage the national security of a foreign country.

85. Given that the Bill's definition of 'public infrastructure' extends to infrastructure that is privately operated, shouldn't there be a defence available for conduct undertaken on behalf of the private company (in addition to conduct in a person's capacity as a public official)?

The sabotage offences contain one specific defence in section 82.10 which applies where the person's conduct was accessing or using a computer or other electronic system in the person's capacity as a public official.

This could be broadened to cover conduct undertaken on behalf of a private owner.

86. Why is there no defence of acting in good faith, similar to the defence in s. 24F of the Crimes Act 1914?

Scenario: A contract electricity professional is asked to carry out major work on a privately owned electricity substation that provides electricity to the public. The contractor is aware of the importance of the electricity substation and is aware that the work has potential to damage the electricity substation. The upgrade causes wide-ranging damage to the electricity substation. As the contractor is working on behalf of a private company that owns the infrastructure, there is no defence available.

Scenario: An IT professional has written to an Australian Government Department for a year pointing out that a vulnerability he has found in software has not been fixed. Frustrated by what he sees as government inaction he exploits this vulnerability to 'prove' to the bureaucracy that he is correct. He has no nefarious intent and is acting in good faith.

The sabotage offences only apply where a person intended to prejudice Australia's national security or advantage the national security of a foreign country (or, in relation to sections 82.7 and 82.8, to

harm or prejudice Australia's economic interests, disrupt the functions of government or damage public infrastructure). A good faith defence is not appropriate.

87. Could the breadth of the sabotage offences impact lawful dissent and protest?

The sabotage offences only apply where a person intended to prejudice Australia's national security or advantage the national security of a foreign country (or, in relation to sections 82.7 and 82.8, to harm or prejudice Australia's economic interests, disrupt the functions of government or damage public infrastructure). The burden will be on the prosecution to prove these elements beyond a reasonable doubt.

88. Could blockading Parliament House, picketing at an MP's office or picketing outside a piece of public infrastructure that results in people who normally enter these places being unable to do so result in a prosecution for a sabotage offence?

Scenario: A group decides to blockade Parliament House, picket an MP's office and protest at a large utility. During the course of their action(s) people who would ordinarily be entitled to access these pieces of public infrastructure are unable to do so.

The sabotage offences only apply where a person intended to prejudice Australia's national security or advantage the national security of a foreign country (or, in relation to sections 82.7 and 82.8, to harm or prejudice Australia's economic interests, disrupt the functions of government or damage public infrastructure). The burden will be on the prosecution to prove these elements beyond a reasonable doubt.

89. Given the incitement, conspiracy and attempt provisions contained in Part 2.4 of the Criminal Code, why is this offence necessary?

Preparatory offences in Commonwealth legislation are generally reserved for serious criminal conduct warranting criminalisation at the preparation stage.

This offence will give law enforcement authorities the means to deal with preparatory conduct, without the need to wait until a sabotage offence is committed or essential public services are put at risk.

Liability for attempt arises from conduct that is 'more than merely preparatory' (subsection 11.1(2) of the Criminal Code). The proposed offence targets conduct that occurs before liability for attempt would arise. The preparatory offence criminalises conduct that would not yet amount to an attempt to commit a sabotage offence.

An offence of attempt carries the same penalty as the primary offence. In recognition of the nature of the preparatory offence, it carries a lower penalty than that applying to the primary sabotage offences.

90. Could suggesting via social media or email:

a. engaging in blockading Parliament House;

b. picketing at an MP's office;

c. picketing outside a piece of public infrastructure; or,

d. a DoS attack designed to disrupt the function of Government

e. result in a prosecution under section 82.9 of the Bill?

The preparation and planning offence at section 82.9 requires proof that a person is engaging in conduct with the intention of preparing for, or planning, an offence against Division 82.

The sabotage offences in Division 82 only apply where a person intended to prejudice Australia's national security or advantage the national security of a foreign country (or, in relation to sections 82.7 and 82.8, to disrupt the functions of government or damage public infrastructure).

Therefore, the prosecution will need to prove that the person engaged in conduct and did so with the intention to prepare or plan for an offence which would result in damage to public infrastructure with the accused intending or reckless as to prejudicing Australia's national security or advantaging the national security of a foreign country. In relation to sections 82.7 and 82.8, the prosecution will need to prove that the person engaged in conduct and did so with the intention to prepare or plan for an offence which would result in the introduction of a vulnerability to public infrastructure with the accused intending or reckless as to harming or prejudicing Australia's economic interests, disrupting the functions of government or damaging public infrastructure).

91. Do any of the definitions in the 'introducing vulnerability offences' extend to individual mobile phones, laptops or tablets?

Mobile phones, laptops and tablets would fall within the scope of the terms 'article' and/or 'thing' for the purposes of sections 82.7 and 82.8 of the Bill.

92. Unlike other sabotage offences, s. 82.7 and 82.8 do not require the person to intend or be reckless as to whether their conduct will prejudice Australia's national security, or advantage another country's national security. The offence will be made out if the person intended or was reckless as to whether their conduct will harm or prejudice Australia's economic interests; disrupt government functions; or damage public infrastructure (s. 82.7 and 82.8).

Scenario: An animal rights organisation, upset with Australia's live animal exports, introduces a vulnerability to the Department of Agriculture and Water Resources' IT systems that slows down animal exports. Whilst there is no suggestion that the group was planning to prejudice Australia's national security, it is alleged the group was seeking to create harm or prejudice to Australia's economic interests. The penalty for this action is 10 years.

a. Was this deliberate?

The sabotage offences in sections 82.7 and section 82.8 will apply if a person engages in the conduct with the intention to prejudice Australia's national security (subparagraph 82.7(d)(i)) or is reckless as to whether his or her conduct would prejudice Australia's national security (subparagraph 82.8(d)(i)).

b. Why is there an additional inclusion of 'harm or prejudice to Australia's economic interests' in sections 82.7 and 82.8 of the Bill, when compared to the other sabotage offences?

The sabotage offences in sections 82.3 to 82.6 require a person to have actually damaged public infrastructure. The prosecution will have proved that the person was reckless as to this element when proving the damage to public infrastructure. Therefore, it is not necessary to also prove that the person intended to disrupt government services or harm Australia's economic interests.

This is not the case with the offences in sections 82.7 and 82.8 where damage has not necessarily yet occurred, but a vulnerability has been created. Therefore, these offences have a broader range of matters listed in relation to the person's intention at the point that he or she introduced the vulnerability.

c. Given that that prejudice is 'not required to be serious or substantial'—is the conduct captured by these offence proportionate to the penalties (10-15 years imprisonment)?

Consistent with Commonwealth criminal law policy, the maximum penalty for an offence should be set appropriately for the worst case scenario.

The justification for the penalty for section 82.7 is set out at paragraph 353 of the Explanatory Memorandum, extracted below:

> The offence will be punishable by a maximum penalty of 15 years imprisonment. The commission of this offence would have serious consequences for Australia's national security and economic interests. It is unacceptable for persons to enable the misuse, impairment or unauthorised access or modification of an article, thing or software that is or is part of public infrastructure. In the worst case scenario, Australians could be killed or seriously harmed as a result of the modification or impairment of public infrastructure by a person intending to harm Australia's national security. This justifies the serious maximum penalty for the offence.

The justification for the penalty for section 82.7 is set out at paragraph 353 of the Explanatory Memorandum, extracted below:

> The offence will be punishable by a maximum penalty of 10 years imprisonment. The commission of this offence would have serious consequences for Australia's national security and economic interests. It is unacceptable for persons to enable the misuse, impairment or unauthorised access or modification of an article, thing or software that is or is part of public infrastructure. In the worst case scenario, Australians could be killed or seriously harmed as a result of the modification or impairment of public infrastructure by a person who is reckless as to the harm that may result. This justifies the serious maximum penalty for the offence.

d. Could these offences be separated?

The offences have already been separated based on whether a person intends to, or is reckless as to whether his or her conduct will, prejudice Australia's national security, harm or prejudice Australia's economic interest, disrupt the functions of government or damage public infrastructure.

The department does not consider further separation to be necessary.

93. *At paragraph four, the Explanatory Memorandum refers to Bill's intent to protect 'critical infrastructure'. However, the Bill creates offences that relate to the more broadly defined term of 'public infrastructure'. Why is this different terminology used?*

The Explanatory Memorandum uses the term 'critical infrastructure' because this is a commonly used and understood term in public discourse.

The term 'public infrastructure' was adopted in the Bill as the best technical description for the matters covered by the definition. This was a drafting matter.

94. *If the Bill is targeting protection of critical infrastructure, why is it not constrained to critical infrastructure as defined in the Security of Critical Infrastructure Bill 2017?*

The purpose of the Bills is quite different and it is not necessary for the definitions to completely align. The harm that comes from damage to public infrastructure due to sabotage is deserving of criminalisation on its own merits.

The Security of Critical Infrastructure Bill is targeted at specific assets and sectors where the risk from espionage, sabotage and coercion is highest. It is designed to ensure that Government has all the necessary information to conduct risk assessments and the powers to enforce mitigations if they are not implemented through collaboration. Given it is imposing a regulatory burden, it is drafted with a narrower focus.

95. *Will the 'introducing vulnerability' offences sufficiently cover cyber security? What agencies were consulted?*

The offences at sections 82.7 and 82.8 will apply to all persons and can be committed online.

The issue of consultation is addressed at Question 1.

96. *Why is there no offence for introducing vulnerability on behalf of a foreign principal?*

The department does not object to the inclusion of the inclusion of an additional offence of introducing a vulnerability that applies where the conduct is engaged in on behalf of a foreign principal. This offence would require a more serious penalty than that applying to section 82.7.

97. *Consequential amendments in the Bill will enable the Minister to order the deportation of a permanent resident who has resided in Australia since childhood, if that person commits an offence of sabotage or introducing vulnerability to public infrastructure. Some of these offences only require 'recklessness' as the requisite state of mind. One offence (s. 82.8) can be established where a person is reckless as to whether damage to 'public infrastructure' would occur. There is no requirement to intend to prejudice national security. Was this intended? Is this consistent with the other offences specified by section 203 of the Migration Act?*

It is important to note that all offences in the Bill require proof of an intention to engage in the relevant conduct. Recklessness only applies to the circumstances in which the offence occurs, or the result of the conduct.

The sabotage offence under section 24AB of the Crimes Act is currently listed as a serious offence for the purposes of section 203 of the *Migration Act 1958*. The Bill repeals this offence, and updates the reference in section 203 of the Migration Act to refer to all of the new offences in Division 82.

The department considers all of the sabotage offences in Division 82 to be serious, as reflected in the maximum penalties applied to the offences.

98. Why are sabotage offences included in the amendments to section 203, but espionage offences are not?

The intention of the amendments to the Migration Act was to ensure that section 203 reflects the changes made in this Bill to the offences currently listed in that section.

Any expansion of the offences covered by section 203 is a matter for the Government.

99. Is it envisaged that there will be circumstances in which a person is convicted of a sabotage offence, but is not a 'threat to security' (within the meaning of section 203)?

a. If so, what is the policy rationale for deporting such a person?

b. If not, would the Minister benefit from ASIO advice? (i.e. an ASA)

The Bill does not affect the operation of section 203 of the Migration Act. The department is unable to comment on the application of this provision in practice.

100. ASIO is able to issue security assessments to assess whether a person engaged in sabotage is a threat to security. Would ASIO be able to issue such an assessment in circumstances where a person has been convicted of a sabotage offence?

ASIO is able to furnish security assessments to a Minister, Commonwealth or State agency in relation to whether certain *prescribed administrative action* should be taken in respect of a person on security grounds. A security assessment may be furnished in circumstances where ASIO assesses it is consistent with the requirements of security for *prescribed administrative action* to be taken in respect of a person; or the requirements of security make it necessary or desirable for *prescribed administrative action* to be taken in respect of the person.

Should ASIO assess a person to be a risk or threat to security, ASIO could furnish an assessment recommending particular *prescribed administrative action* be taken. *Prescribed administrative action* is defined in section 35 of the ASIO Act, and could include action in relation to:

- the grant, refusal or cancellation of a security clearance;
- the grant, refusal or cancellation of an Aviation Security Identification Card (ASIC) or Maritime Security Identification Card (MSIC);
- the grant, refusal or cancellation of an Australian visa;
- the grant or refusal of Australian citizenship;

- the grant, refusal or cancellation of an Australian travel document.

Theft of trade secrets offence

101. Why is necessary for 'theft of trade secrets' issue to be dealt with by way of a criminal offence, rather than civil measures?

a. Is there a chance that the publicity of a criminal trial may prevent victims of this kind of offence from coming forward?

b. If there is a criminal trial, how might owners of trade secrets compensated?

The department considers it appropriate to criminalise the theft of trade secrets where it is done on behalf of a foreign government principal. This amounts to economic espionage, which is harmful to Australia's national security and economic prosperity.

The Bill does not criminalise theft of trade secrets where a foreign government is not involved. This is more appropriately left to civil enforcement mechanisms or state/territory theft offences.

The goal of the offence is to protect persons or companies who have been the victims of such activity when undertaken on behalf of a foreign government.

In terms of compensation, section 21B of the Crimes Act allows a sentencing court to make an order requiring an offender to make reparation to any person, by way of money payment or otherwise, in respect of any loss suffered, or any expense incurred, by the person by reason of the offence.

Treason

102. Both the existing and the amended treason offence in the Bill provide that a person commits the offence if they 'materially assist' an enemy. However, this term is not defined.

a. Why does the language in this offence not align with the similar Criminal Code offence of 'Providing support to a terrorist organisation' (s.102.7), which refers to 'provides to an organisation support or resources'?

b. Could 'materially assist' be interpreted to extend to indirect assistance, such as providing humanitarian assistance or refusing to fight?

c. Is there any reason why 'materially assist' could not be defined in the Bill?

The use of the term 'materially assist' is consistent with existing treason offences. It has been retained as it is a high threshold for the assistance that must be provided in order for a treason offence to be committed. It is a higher threshold than that found in the offence relating to terrorist organisations at section 102.7, which is considered appropriate given the severe penalty applying to treason offences.

The Explanatory Memorandum explains the term 'materially assist' at paragraph 158, extracted below:

> For paragraph 80.1AA(1)(d), the prosecution will have to prove beyond a reasonable doubt that the person intended that his or her conduct would materially assist the enemy to engage in armed conflict involving the Commonwealth or the Australian Defence Force. The term 'materially assist' is not defined and will be given its ordinary meaning. It is intended that this term will cover assistance in the form of money or practical goods, and that the assistance will have to be more than merely trivial in order to 'materially' assist. The conduct must also be intended to materially assist the enemy in armed conflict.

A defence is available for people who engaged in conduct solely by way of, or for the purposes of, the provision of aid or assistance of a humanitarian nature (subsection 80.1AA(4)).

103. Both the existing and the amended treason offences apply to 'residents of Australia'. Does the term 'resident' only extend to permanent residents, or is it intended to extend to persons staying in Australia on a temporary visa, for example a student visa, business visa or tourist visa? If so, do these persons owe an allegiance to Australia sufficient to engage in treason?

The Bill is not limited to permanent residents. A person who is voluntarily temporarily resident in Australia would be considered to have 'voluntarily put himself or herself under the protection of the Commonwealth'.

Treachery

104. The Bill proposes to extend the treachery offence to the use of force or violence to overthrow the 'lawful authority of the Government of the Commonwealth'. What is meant by the term 'lawful authority' (please provide examples covering the full scope of this term)? Could the term be defined in the Bill?

The term 'lawful authority of the Commonwealth' is used for consistency with the existing offence of urging violence against the Constitution in section 80.2 of the Criminal Code.

Paragraph 185 of the Explanatory Memorandum provides the following information about the meaning of this term.

> For paragraph 80.1AC(1)(c), the prosecution will have to prove beyond a reasonable doubt that the person engaged in his or her conduct with the intention of overthrowing the Constitution, the Government of the Commonwealth or a State or Territory or the lawful authority of the Government of the Commonwealth. This could include the overthrow of an arm of the Government. If a person intended to overthrow the Executive Government then this will be sufficient even if they do not intend to overthrow the Parliament or the judiciary. The application of intention to this result element means that the prosecution will have to prove that the person means to bring about the overthrow or is aware that it will occur in the ordinary course of events.

105. Have intimidation and threats been purposely excluded from the proposed treachery offence, in contrast to the proposed 'interference with political rights and duties' offence in clause 83.4? If so, why?

The use of the term 'force or violence' picks up on the language used in the existing treachery offence at subparagraph 24AA(1)(a)(ii) of the Crimes Act. It is also consistent with the language used

in the existing offence of urging violence against the Constitution in section 80.2 of the Criminal Code (see paragraph 80.2(1)(a)).

Conversely, the references to intimidation and threats in new section 83.4 of the Bill pick up on the existing language used in section 28 of the Crimes Act.

Given that a penalty of life imprisonment applies to the treachery offence at subsection 80.1AC of the Bill, it is considered appropriate that the offence be limited to conduct involving force or violence and not extend to conduct involving intimidation or threats.

Other threats to security

106. Could peace campaigners, advocating ADF members to not follow orders, be captured by the 'advocating mutiny' offence?

Scenario: An Australian warplane in the Middle East has been found to have accidentally bombed civilians. A peace group and some individuals campaigning against Australia's involvement in this operation make statements to the effect that 'ADF personnel should not follow their orders, as they risk becoming war criminals'

In order for the advocating mutiny offence at section 83.1 to apply, a person must be reckless as to whether:

- the conduct involves advocating mutiny, and
- the result will be that a defence member will take part in a mutiny.

This requires the prosecution to prove, beyond a reasonable doubt, that the person was aware of a substantial risk that the conduct involves advocating mutiny that the result will be that a defence member will take part in a mutiny and that, having regard to the circumstances known to him or her, it was unjustifiable to take the risk.

The department is not able to provide a definitive answer in relation to hypothetical scenarios as each case will depend on its facts and circumstances, as well as the admissible evidence.

107. Why has the penalty for' military style training involving foreign government principal' been increased to 20 years imprisonment from the five years contained in s. 27 (unlawful drilling) of the Crimes Act 1914?

Paragraph 495 of the Explanatory Memorandum, extracted below, justifies the increased penalty for this offence:

> The maximum penalty of 20 years imprisonment is comparable with maximum penalties for offences for providing or receiving training connected to terrorist acts which carry penalties of 15 and 25 years imprisonment. The maximum penalty is appropriate to recognise the serious harm to Australia's sovereignty, national security and other defence interests that could result from the provision and receipt of military style training by a foreign government principal.

108. Why has the penalty for 'interference with political rights and duties' been increased to 10 years imprisonment from the three years contained in section 28 (interference with political liberty) of the Crimes Act 1914?

Paragraph 533 of the Explanatory Memorandum, extracted below, justifies the increased penalty for this offence:

> The maximum penalty of ten years imprisonment is appropriate and appropriately criminalises conduct involving force or violence that interferences with a person's exercise of their democratic or political rights or duties.

The right to engage in Australia's democratic and political processes is essential to Australia's free and open society. Conduct that interferes with these rights and involves the use of force, violence, intimidation or threats is a grave threat to Australia's democracy and stifles the kind of open debate which is fundamental to Australia's society.

109. Why have the penalties for 'inciting mutiny' and 'assisting prisoners of war to escape' been reduced (from life down to seven and 15 years respectively)?

Paragraphs 443 and 444 of the Explanatory Memorandum, extracted below, justify the penalty for the offence of advocating mutiny at section 83.1 of the Bill.

> Section 83.1 replaces section 25 of the Crimes Act which carries a maximum penalty of life imprisonment. Section 25 of the Crimes Act was enacted in the original Crimes Act in 1914 and the penalty of life imprisonment does not reflect contemporary standards. It is not appropriate for an offence of advocating mutiny (especially where committed by a civilian rather than a defence member) to carry the same penalty as the most serious mutiny offence applying to defence members (subsection 20(2) of the Defence Force Discipline Act).
>
> The maximum penalty of seven years imprisonment is consistent with maximum penalties for the Criminal Code offences of urging violence (section 80.2) and advocating genocide (section 80.2D), which also carry maximum penalties of seven years imprisonment.

Paragraphs 469 of the Explanatory Memorandum, extracted below, justifies the penalty for the offence of advocating mutiny at section 83.1 of the Bill.

> Section 83.2 replaces section 26 of the Crimes Act which carries a maximum penalty of life imprisonment. Section 26 of the Crimes Act was enacted in the original Crimes Act in 1914 and the existing penalty of life imprisonment does not reflect contemporary standards of seriousness. The maximum penalty of 15 years imprisonment is comparable with maximum penalties for offences relating to escaping criminal detention. For example, section 47A of the Crimes Act specifies a maximum penalty of 14 years imprisonment for the offence of rescuing a prisoner from criminal detention.

Consequential amendments

110. The Bill proposes substituting references to sabotage and espionage in s. 35A of the Australian Citizenship Act 2007 with all of the proposed offences in Division 82 (Sabotage) and Division 91 (Espionage). These offences are significantly broader in scope and do not require the offender to intend to harm or prejudice national security. For example, introducing a vulnerability

to public infrastructure, reckless as to whether damage to public infrastructure would occur (s. 82.8(d)(iv)); or dealing in information concerning national security (s.91.3) Was this intended? If so, could this be addressed in the Explanatory Memorandum?

The department was aware that this would be the effect of the consequential amendment to the *Australian Citizenship Act 2007*. The Explanatory Memorandum states that the amendment will ensure that the definition of 'national security offence' would continue to cover espionage and sabotage following the enactment of the new offences (see paragraph 1223).

The fact that espionage and sabotage offences are broadened is clear on the face of the Bill. The Explanatory Memorandum could more explicitly state that this effect was intended if the Committee would consider this useful.

111. Why do the amendments include all of the proposed offences in new Division 82 (Sabotage) and Division 91 (Espionage), rather than be limited to the most serious of the sabotage and espionage offences? If this was intended, could the Minister possess a discretion to approve a citizenship application where the applicant has been convicted of one of the less serious sabotage or espionage offences proposed in new Division 82 and new Division 91 of the Criminal Code?

The scope of espionage and sabotage offences is a matter for the Parliament. The policy intention of the consequential amendments to the *Australian Citizenship Act* is to ensure that the scope of section 35A of the Australian Citizenship Act aligns with the scope of the enacted offences, as determined by the Parliament.

112. Do these amendments fulfil Australia's obligations under the 1954 Convention relating to the Status of Stateless Persons. In particular, would all persons convicted of one of the proposed offences be considered to fall outside the scope of the Convention, by reference to the criteria set out in Article 1(2)(iii)? For example, a person convicted of an offence under s. 82.8 with a recklessness as to 28.7(d)(iv).

Australia is party to two conventions on statelessness: the Convention relating to the Status of Stateless Persons[2] (1954 Status Convention) and the Convention on the Reduction of Statelessness (1961 Reduction Convention).[3]

The 1954 Status Convention establishes minimum standards of treatment of stateless persons. For example, the Convention guarantees stateless persons access to courts and provides that stateless persons are to enjoy, at a minimum, the same treatment as nationals with respect to freedom of religion. The Convention is not relevant to the Bill because the Bill does not involve any proposals to change the way in which stateless persons are treated in Australia.

The 1961 Reduction Convention imposes obligations on State parties directed at reducing the incidence of statelessness. In particular, it contains a range of obligations related to the conferral and withdrawal of citizenship. These obligations are relevant to the Bill to the extent that the Bill

[2] [1974] ATS 20, in force generally 6 June 1960, and for Australia, 13 March 1974.
[3] [1975] ATS 46, in force generally and for Australia, 13 December 1975.

makes changes to offences in the Criminal Code and Crimes Act for which a conviction may, under the *Australian Citizenship Act 2007* (Cth), operate as a bar to the grant of citizenship or as a ground for cessation of citizenship.

The department will consider further the interaction between the Bill and Australia's obligations under the 1961 Reduction Convention.

Aggravated offence for giving false or misleading information – security vetting

113. Is the aggravated offence in Schedule 3 for knowingly providing false or misleading information (or withholding information), intended to apply only to the person applying for a security clearance, or to all persons involved in the process? For example, would the aggravated offence extend to family members and personal referees?

The offence in section 137.1A will apply to any person who provides false or misleading information to the Commonwealth in relation to an application for, or maintenance of, an Australian Government security clearance. Protecting the integrity of security vetting is of fundamental importance and referee checking is a key element of the vetting process.

The ability of a person to select referees who would knowingly provide false or misleading information is likely to gravely compromise the vetting process.

In order to commit the underlying offence at section 137.1 of the Criminal Code, the person will need to know that the information is false or misleading or omits any matter or thing without which the information is misleading.

For paragraph 137.1A(1)(b), the person will need to be reckless about the fact that the information was given in relation to an application for, or the maintenance of, an Australian Government security clearance. This will require proof that the person was aware of a substantial risk that the information was given in relation to such a process and, having regard to the facts and circumstances known to him or her, it is unjustifiable to take the risk.

The department notes that the defence in subsections 137.1(4) to (6) of the underlying offence will apply to the commission of the aggravated offence. This defence applies if the person or Commonwealth entity to whom the information is given did not take reasonable steps to inform the person of the existence of the offence of providing false or misleading information.

Amendments to the Foreign Influence Transparency Scheme

114. Why are the amendments to the FITS Bill contained in a Schedule to the EFI Bill, and not as part of the FITS Bill?

Paragraph 1763 of the Explanatory Memorandum, extracted below, explains why the amendments to the Foreign Influence Transparency Scheme Act 2017 are included in the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017.

> The usual practice is to not have amending Schedules at the ends of Bill that establish new Principal Acts. In accordance with this practice, Schedule 5 has been included in this amending Bill rather than as a schedule to the Foreign Influence Transparency Scheme Bill 2017.

This is a matter of drafting practice.

115. Why are political campaigners, a concept which will be created by the Electoral Legislation Amendment (Electoral Funding and Disclosure Reform) Bill 2017, treated the same as a political campaigner under the FITS Bill? If the definition of political campaigner is amended, what impact will this have on the Scheme?

Paragraphs 1772 to 1776 of the Explanatory Memorandum, extracted below, justify the extension of the Foreign Influence Transparency Scheme to 'political campaigners'.

> This item amends the definition of 'general political lobbying' set out at section 10 of the *Foreign Influence Transparency Scheme Act 2017*. The item inserts new paragraph (e), which reads 'a person or entity that is registered under the *Commonwealth Electoral Act 1918* as a political campaigner'. The effect of this insertion is that the definition of 'general political lobbying' is expanded to cover circumstances where a person lobbies a registered political party. If a person lobbies a registered political campaigner this may make the person liable to register under the Foreign Influence Transparency Scheme. Whether a person is liable will depend on whether the general political lobbying is undertaken on behalf of a foreign principal, the purpose for which the lobbying is undertaken, and whether or not an exemption applies.
>
> Under the Commonwealth Electoral Act, a person or entity must register as a political campaigner if their political expenditure during the current, or in any of the previous three, financial years was $100,000 or more. A person or entity must also register as a political campaigner if their political expenditure during a financial year is $50,000 or more, and that amount is at least 50 per cent of their allowable amount (as defined under the Commonwealth Electoral Act) for the year.
>
> Registered political campaigners have been included under the definition of 'general political lobbying' because lobbying such persons or entities is an inherently political activity. For example:
>
> Group X is a registered political campaigner under the Commonwealth Electoral Act. Group X has a membership of 1 million Australians, and has a significant funding base. Group X conducts campaigns which are specifically designed to influence public opinion on federal government policies. In the past, a number of Group X's campaigns have had a direct effect on political parties changing their policy platforms.
>
> Given the position of influence held by registered political campaigners within the Australian political system, it is important that the Foreign Influence Transparency Act extend to foreign influence over such persons and entities.

The commencement of these amendments is dealt with in Item 7 of the table in Item 2 of the Bill. Paragraphs 122 and 123 of the Explanatory Memorandum, extracted below, explain the commencement provision.

> Schedule 5, Part 2 commences on the later of:
>
> - immediately after the commencement of the *Foreign Influence Transparency Scheme Act 2017*, and

- immediately after the commencement of Part 1 of Schedule 1 to the *Electoral Legislation Amendment (Electoral Funding and Disclosure Reform) Act 2017*.

However, if both of the events listed above do not occur then Part 2 of Schedule 5 will not commence at all.

Under Item 3 of Part 2 of Schedule 5, a 'political campaigner' will be defined in the *Foreign Influence Transparency Scheme Act* by reference to the definition in the *Commonwealth Electoral Act 1918*. The definitions will therefore remain consistent, even if the definition of 'political campaigner' in the Commonwealth Electoral Act is amended.