2016 - 2017

THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

HOUSE OF REPRESENTATIVES

NATIONAL SECURITY LEGISLATION AMENDMENT (ESPIONAGE AND FOREIGN INTERFERENCE) BILL 2017

EXPLANATORY MEMORANDUM

(Circulated by authority of the
Attorney-General, Senator the Honourable George Brandis QC)

NATIONAL SECURITY LEGISLATION AMENDMENT (ESPIONAGE AND FOREIGN INTERFERENCE) BILL 2017

GENERAL OUTLINE

1. This Bill amends the *Criminal Code Act 1995, Crimes Act 1914* and *Telecommunications (Interception and Access) Act 1979* and makes consequential amendments to other legislation.

2. Espionage and foreign interference pose significant risks to Australia's security and defence. Foreign adversaries are actively working against Australia's interests through a variety of means, including obtaining classified information or seeking to influence the outcome of Australia's democratic processes.

3. Activities undertaken by foreign adversaries, and those acting on their behalf, can cause severe harm to Australia's national security, compromising Australia's military capabilities and alliance relationships, and can pose a grave threat to Australia's economic stability and well-being. By wielding undue influence on the Australian political landscape, foreign adversaries have the potential to undermine Australia's sovereignty and system of government.

4. The Bill will comprehensively reform key offences dealing with threats to national security, particularly those posed by foreign principals. The Bill:

- strengthens existing espionage offences
- introduces new foreign interference offences targeting covert, deceptive or threatening actions by foreign actors who intend to influence Australia's democratic or government processes or to harm Australia
- reforms Commonwealth's secrecy offences, ensuring they appropriately criminalise leaks of harmful information while also protecting freedom of speech
- introduces comprehensive new sabotage offences that effectively protect critical infrastructure in the modern environment
- modernises and reforms offences against government, including treason, to better protect Australia's defence and democracy
- introduces a new theft of trade secrets offence to protect Australia from economic espionage by foreign government principals,
- introduces a new aggravated offence for providing false and misleading information in the context of security clearance processes, and
- ensures law enforcement agencies have access to telecommunications interception powers to investigate these serious offences.

5. Schedule 1 amends Part 5.1 of the Criminal Code to modernise Australia's treason offences. It will ensure that treason offences appropriately reflect modern terminology

related to armed conflict. The amendments to Part 5.1 will also create a new offence of treachery in the Criminal Code (replacing the existing archaic and antiquated treachery offence in section 24AA of the Crimes Act) that applies where a person seeks to use force or violence to overthrow the Constitution or an Australian government.

6. Schedule 1 introduces comprehensive sabotage offences into new Division 82 in Part 5.1 of the Criminal Code, replacing the existing sabotage offence at section 24AB of the Crimes Act, which only protects Defence facilities. The new sabotage offences will criminalise conduct causing damage to a broad range of critical infrastructure where it could prejudice Australia's national security. The offences in new Division 82 will apply higher penalties where sabotage offences are committed on behalf of foreign principals.
New Division 82 will also contain offences that apply where a person's conduct does not immediately cause damage, but leaves an item or system vulnerable to future misuse or exploitation.

7. Schedule 1 introduces new Division 83 into Part 5.1 of the Criminal Code.
Division 83 will modernise and improve the existing offences against government in Part II of the Crimes Act (which will be repealed). The offences in Division 83 criminalise threats to Australia's security, including advocating mutiny, assisting prisoners of war to escape and military-style training for a foreign government. New Division 83 also criminalises the use of force, violence or intimidation to interfere with Australian democratic or political rights.

8. Schedule 1 amends Part 5.2 of the Criminal Code to introduce comprehensive new espionage offences in Division 91. The new offences criminalise a broad range of dealings with information, including possessing or receiving, and protect a broader range of information, including unclassified material. The current methodology of Australia's adversaries means that dealings with unclassified information, if accompanied by the requisite intention to harm Australia, can be as damaging as the passage of classified information. The new offences will not just target the person who discloses the information, but also the actions of the foreign principal who receives the information. The new offences in Division 91 will also, for the first time, criminalise soliciting or procuring a person to engage in espionage and will introduce a new preparation or planning offence, which will allow law enforcement agencies to intervene at an earlier stage to prevent harmful conduct occurring.

9. Schedule 1 introduces new Division 92 into Part 5.2 of the Criminal Code which will contain new foreign interference offences. These offences complement the espionage offences by criminalising a range of other harmful conduct undertaken by foreign principals who seek to interfere with Australia's political, governmental or democratic processes, to support their own intelligence activities or to otherwise prejudice Australia's national security. The offences will apply where a person's conduct is covert or deceptive, involves threats or menaces or does not disclose the fact that conduct is undertaken on behalf of a foreign principal. New Division 92 also criminalises the provision of support or funding to foreign intelligence agencies.

10. Schedule 1 introduces new Division 92A into Part 5.2 of the Criminal Code which contains a new offence targeting theft of trade secrets on behalf of a foreign government. This amounts to economic espionage and can severely damage Australia's national security and economic interests. The new offence will apply to dishonest dealings with trade secrets on behalf of a foreign government principal.

11. Schedule 2 introduces new Part 5.6 and Division 122 into the Criminal Code. New Part 5.6 contains a suite of new Commonwealth secrecy offences. These new offences replace sections 70 and 79 of the Crimes Act and will apply if the information disclosed is inherently harmful (such as security classified information) or would otherwise cause harm to Australia's interests. The offences will apply to all persons, not just Commonwealth officers. New Division 122 includes defences to ensure the offences do not apply too broadly, including a defence specifically applying to journalists engaged in fair and accurate reporting in the public interest. The offences ensure harmful information cannot be released, while appropriate defences protect freedom of speech.

12. Schedule 3 amends Division 137 of Part 7.4 of the Criminal Code to introduce a new aggravated offence that applies where a person provides false or misleading information in relation to an Australian Government security clearance process. This reflects the serious consequences that can flow from the provision of misleading information, or the omission of relevant information, during a security clearance process.

13. Schedule 4 amends the *Telecommunications (Interception and Access) Act 1979* to ensure the powers under that Act are available to investigate the offences contained in the Bill.

14. Schedule 5 makes amendments relevant to the Foreign Influence Transparency Scheme. Transitional amendments address pre-existing arrangements with foreign principals at the time of commencement of the Foreign Influence Transparency Scheme Act. Other amendments reflect the interaction between the *Foreign Influence Transparency Scheme Act 2017* and the *Electoral Legislation Amendment (Electoral Funding and Disclosure Reform) Act 2017*.

FINANCIAL IMPACT

2. The amendments in this Bill have no financial impact on Government revenue.

ACRONYMS

Acts Interpretation Act	*Acts Interpretation Act 1901*
AFP	Australian Federal Police
ALRC	Australian Law Reform Commission
ASIO	Australian Security Intelligence Organisation
ASIO Act	*Australian Security Intelligence Organisation Act 1979*
Australian Citizenship Act	*Australian Citizenship Act 2007*
Australian Federal Police Act	*Australian Federal Police Act 1979*
CDPP	Commonwealth Director of Public Prosecutions
Commonwealth Electoral Act	*Commonwealth Electoral Act 1918*
Crimes Act	*Crimes Act 1914*
Criminal Code	*Criminal Code Act 1995*
Defence Act	*Defence Act 1903*
Defence Force Discipline Act	*Defence Force Discipline Act 1982*
Guide to Framing Commonwealth Offences	*Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*
ICRC	International Committee of the Red Cross
NSI Act	*National Security Information (Criminal and Civil Proceedings) Act 2004*
POCA	*Proceeds of Crime Act 2002*
PID Act	*Public Interest Disclosure Act 2013*
Telecommunications Act	*Telecommunications Act 1997*
TIA Act	*Telecommunications (Interception and Access) Act 1979*
UN	United Nations

STATEMENT OF COMPATIBILITY WITH HUMAN RIGHTS

Prepared in accordance with Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011

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

15. This Bill is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.

Overview of the Bill

16. The National Security (Espionage and Foreign Interference) Bill 2017 (the Bill) amends the *Criminal Code Act 1995*, the *Crimes Act 1914* and the *Telecommunications (Interception and Access) Act 1979* in response to the Government's review of Australia's espionage and foreign interference laws. The Bill will modernise and strengthen espionage, secrecy and related laws, and create new foreign interference laws to ensure the protection of Australia and Australia's interests.

17. Outlined below is a brief summary of the substantive changes to each of the relevant Acts.

Criminal Code Act 1995

18. The Bill:

- strengthens existing espionage offences
- introduces new foreign interference offences targeting covert, deceptive or threatening actions by foreign actors who intend to influence Australia's democratic or government processes or to harm Australia
- reforms Commonwealth's secrecy offences, ensuring they appropriately criminalise leaks of harmful information while also protecting freedom of speech
- introduces comprehensive new sabotage offences that effectively protect critical infrastructure in the modern environment
- modernises and reforms offences against government, including treason, to better protect Australia's defence and democracy
- introduce a new theft of trade secrets offence to protect Australia from economic espionage by foreign government principals, and
- introduces a new aggravated offence for providing false and misleading information in the context of security clearance processes, and

- ensures law enforcement agencies have access to telecommunications interception powers to investigate these serious offences.

Crimes Act 1914

19. The amendments to the Crimes Act include repealing existing offences relating to secrecy, sabotage and other offences against government in Part II of the Crimes Act and transferring them to the Criminal Code.

Telecommunications (Interception and Access) Act 1979

20. The definition of 'serious offence' in subsection 5D(1) of the TIA Act will be amended so that the powers in the TIA Act to apply to all offences created in the Bill. This ensures law enforcement agencies have access to telecommunications interception powers to investigate these serious offences.

Human rights implications

21. This Bill engages the following rights:

- the prohibition of torture, or cruel, inhuman and degrading treatment or punishment in Article 7 of the *International Covenant on Civil and Political Rights* (ICCPR)
- the right to liberty of person and freedom from arbitrary detention in Article 9(1) of the ICCPR
- the right to trial within a reasonable period or to release in Article 9(3) of the ICCPR
- the right to be tried without undue delay in Article 14(3)(c) of the ICCPR
- the right to be presumed innocent in Article 14(2) of the ICCPR
- the right to privacy in Article 17 of the ICCPR
- the right to opinion and freedom of expression in Article 19 of the ICCPR
- the prohibition on propaganda for war and advocacy of national, racial or religious hatred in Article 20 of the ICCPR
- the right to peaceful assembly in Article 21 of the ICCPR
- the right to freedom of association in Article 22 of the ICCPR, and
- the right to take part in public affairs and the right to vote in Article 25 of the ICCPR.

Human rights promoted by the Bill

Right to liberty and freedom from arbitrary detention

22. Article 9(1) of the ICCPR states that everyone has the right to liberty and security of person and that no one shall be subjected to arbitrary arrest or detention. The Bill engages the right to liberty and freedom from arbitrary detention by requiring consent of the

Attorney-General prior to the prosecution of an offence of espionage, foreign interference, sabotage, theft of trade secrets, or other threats against security.

23. In circumstances in which a person is not arrested or remanded in custody pending a decision of the Attorney-General, the requirement for consent will protect and promote the right to liberty and freedom from arbitrary detention. This is because in deciding whether to consent to the prosecution of an offence the Attorney-General must consider whether the conduct in question was authorised and therefore whether the accused has a defence available. In this respect a proposed prosecution is scrutinised from both the prosecution and defence perspectives, and a judgment made about the appropriateness of the prosecution, having regard to the facts of the case and the scope of authorised conduct provided for in the Bill.

24. This individualised assessment prior to the prosecution may prevent any unwarranted deprivation of liberty thereby safeguarding the rights contained in Article 9(1).

Right to opinion and freedom of expression, right to freedom of assembly and association and right to take part in public affairs and elections

25. Article 19 of the ICCPR states that everyone has the right to hold opinions without interference and that everyone shall have the right to freedom of expression. Article 21 of the ICCPR recognises the right to peaceful assembly while Article 22 provides for the right to freedom of association with others. Article 25 of the ICCPR further states that every citizen shall have the right and the opportunity to take part in the conduct of public affairs, directly or through freely chosen representatives, and to vote and to be elected at genuine periodic elections.

26. The Bill protects and promotes the right to opinion and freedom of expression, the freedom of assembly and association and the right to take part in public affairs and elections by:

- introducing foreign interference offences, which will criminalise certain conduct that seeks to influence the exercise of Australian democratic or political rights, and

- replacing the offence of 'interference with political liberty' with the offence of 'interference with political rights and duties'.

27. Foreign interference offences will criminalise conduct engaged in on behalf of a foreign principal that is covert or involves deception, threats or menaces and which seeks to influence a political or governmental process of an Australian government or the exercise of an Australian democratic or political right. Reference to the exercise of Australian democratic or political rights is intended to cover a broad range of rights held by Australians in relation to participation in Australia's democracy, including voting in elections and referenda and participating in lawful protests, rights which clearly fall within the scope of Articles 19, 21, 22 and 25.

28. Unlike the routine business of diplomatic influence practised by all nation states, foreign interference is characterised by clandestine and deceptive activities undertaken by foreign actors seeking to cause significant harm to Australia's national interests, or to advance their own interests. Foreign interference can erode Australia's sovereignty by

diminishing public confidence in the integrity of Australia's political and government institutions, and undermining Australian societal values. During elections, referendums and plebiscites in particular, foreign interference can undermine the legitimacy or perceived legitimacy of government and its processes, enable the perception of corruption, and obfuscate information that might impact the voting decisions of the public.

29. In addition to foreign interference offences, the Bill creates the offence of 'interference with political rights and duties' which will apply where a person uses force, violence, threats or intimidation to interfere with a person's democratic or political right under the Constitution or Commonwealth law. The term 'Australian democratic or political right' is intended to cover a broad range of rights held by Australians in relation to participation in Australia's democracy, including voting in elections and referenda and participating in lawful protests. The limitation to 'Australian' democratic and political rights is intended to limit the operation of this paragraph to rights that arise because of a person's status as Australian. The limitation to rights which 'arise under the Constitution or a law of the Commonwealth' ties the offence to Commonwealth jurisdiction, excluding rights and duties which arise under state and territory laws. Democratic or political rights which arise under the Constitution or a Commonwealth law may include for example:

- the implied freedom of political communication, and
- the right to vote as provided for in section 41 of the Constitution and in the *Commonwealth Electoral Act 1918*.

30. The implied freedom of political communication and the right to vote clearly engage Article 19 of the ICCPR (right to opinion and freedom of expression) and Article 25 of the ICCPR (right to take part in political affairs and right to vote).

31. As with foreign interference, conduct which interferes with political rights and duties can diminish public confidence in the integrity of Australia's political and government institutions, enable the perception of corruption, and obfuscate information that might impact the voting decisions of the public during election periods. Unlike foreign interference, the offence of interference with political rights and duties requires the use of force, violence, threats or intimidation. In the worst case scenario, people may be killed or seriously harmed as a result of violence used to interfere with a person's democratic or political rights.

32. By criminalising foreign interference and interference with political rights and duties the Bill will prevent the harmful impact that such acts have on Australians and Australia's political and governmental processes. In accordance with the obligations which arise under Article 19 of the ICCPR, these offences will protect Australians from 'any acts by private persons or entities that would impair the enjoyment of the freedoms of opinion and expression.' During elections, the prohibition on foreign interference will ensure the right 'to vote without undue influence or coercion of any kind' while the offence of interference with political rights and duties will ensure persons are 'free to form opinions without the threat of violence, compulsion, inducement or manipulative interference'.

33. On this basis, the Bill will enable the exercise of democratic and political rights and duties without interference (as described) and thereby protect and promote the rights contained in Articles 19, 21, 22 and 25.

Prohibition on propaganda for war and advocacy of national, racial, or religious hatred

34. Article 20 of the ICCPR states that any propaganda for war and any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law. According to the United Nations Human Rights Committee (the Human Rights Committee), the prohibition on propaganda for war extends to all forms of propaganda threatening or resulting in an act of aggression or breach of the peace contrary to the Charter of the United Nations; while the prohibition on advocacy of national, racial or religious hatred constituting incitement to discrimination, hostility or violence occurs regardless of whether such advocacy is internal or external to the State concerned. Article 20 requires States to provide for laws which clearly prohibit propaganda and advocacy as described and which provide for appropriate sanctions in cases of violation.

35. The Bill protects and promotes the prohibitions contained in Article 20 by replacing the existing offence of inciting mutiny with the offence of advocating mutiny and enacting a treachery offence where a person uses force or violence and intends to overthrow the Constitution or an Australian government.

36. The advocating mutiny offence will apply where a person advocates mutiny, reckless as to whether the result will be that a member of the defence force takes part in a mutiny. The term 'advocating' is intended to take its ordinary meaning and could include supporting, recommending, promoting, encouraging, urging and inciting. The term 'mutiny' will be defined as a combination between persons who are, or at least two of whom are, members of the Australian Defence Force (ADF) who overthrow lawful authority in the ADF or in a force of another country that is acting in cooperation with the ADF; or who resist such lawful authority in such a manner as to substantially prejudice the operational efficiency of the ADF or of, or of a part of, a force of another country that is acting in cooperation with the ADF.

37. The treachery offence criminalises the use of force or violence intended to overthrow the Constitution, the Government of the Commonwealth or of a State or Territory or the lawful authority of the government of the Commonwealth. The new treachery offence will carry a penalty of life imprisonment.

38. Conduct which advocates mutiny or involves the use of force or violence to overthrow the government falls within the prohibitions contained in Article 20. By its very nature, overthrow of the defence force or government of Australia would involve hostility and/or violence. Advocating the overthrow of the government or defence force of Australia may also constitute national hatred within the context of Article 20. In this respect, the Bill ensures that the propaganda and advocacy described in Article 20 is clearly prohibited and further ensures appropriate sanctions by providing for a penalty of imprisonment in cases of violation. By replacing the existing offence of 'inciting mutiny' to reflect the modern Australian context, the Bill will further strengthen the prohibitions in Article 20.

Human rights limited by the Bill

Legitimate objective of the Bill

39. Under international human rights law, any limitation on rights and freedoms must be reasonable, necessary and proportionate for the pursuit of a legitimate objective. For an objective to be legitimate, it must address a pressing or substantial concern, and not simply seek an outcome regarded as desirable or convenient.

40. The objective of the Bill is to modernise and strengthen Australia's espionage, foreign interference, secrecy and related laws to ensure the protection of Australia's security and Australian interests. Foreign actors are currently seeking to harm Australian interests on an unprecedented scale, posing a grave threat to Australia's sovereignty, prosperity and national security. This threat is a substantial concern for the Australian Government. If left unchecked, espionage and foreign interference activities may diminish public confidence in the integrity of political and government institutions, compromise Australia's military capabilities and alliance relationships, and undercut economic and business interests within Australia and overseas.

41. Existing laws in Australia are currently inadequate to deter and counter pervasive espionage and foreign interference activities directed against Australian interests. Espionage, secrecy and related criminal offences fail to take into account the current operational environment and technological advances which have provided hostile foreign intelligence services with greater global reach, access to sensitive data and tools to obscure identity. It is essential to expand the scope of the criminal law to cover contemporary methodologies for espionage and foreign interference currently occurring in Australia, as well as to allow for coverage of such methodologies as may be developed in the future. A lack of serious criminal penalties and law enforcement powers has also resulted in a permissive operating environment for malicious foreign actors, in which Australian agencies are unable to effectively disrupt and mitigate threats. Agencies must have the full suite of powers available to them under law to successfully investigate and prosecute acts of espionage and foreign interference.

42. The Bill will achieve its objective in ensuring the protection of Australia's national security by:

- broadening the investigative powers of Australian agencies
- updating existing offences dealing with espionage, secrecy, sabotage and treason, and
- creating new offences to address foreign interference and the theft of trade secrets.

Prohibition of torture, or other cruel, inhuman or degrading treatment or punishment

43. Article 7 of the ICCPR states that no one shall be subjected to torture or to cruel, inhuman or degrading treatment or punishment. The text of the Article 7 allows no limitation.

44. The Bill engages the prohibition on torture, cruel, inhuman or degrading treatment by providing for penalties of imprisonment. Penalties of imprisonment may amount to cruel, inhuman or degrading treatment where their application is disproportionate to the offence committed.

45. The penalties in the Bill have been set at a level that is adequate to deter and punish a worst case scenario, including repeat offences. Responsibility for determining criminal guilt and imposing an appropriate sentence rests with the courts in their exercise of judicial power. The court will have discretion to implement an appropriate penalty based on all of the circumstances of the case. In this regard, the application of the penalties is not disproportionate.

Right to liberty of person and freedom from arbitrary detention

46. Article 9(1) of the ICCPR states that everyone has the right to liberty and security of person and that no one shall be subjected to arbitrary arrest or detention. Under Article 9(3) the right to liberty extends to the right to be tried within a reasonable period or to be released. Limitations on the right to liberty are permitted to the extent that they are 'in accordance with such procedures as are established by law', provided that the law and the enforcement of it is not arbitrary, and where they are reasonable, necessary and proportionate to achieve a legitimate objective. The Bill limits the right to liberty of a person and freedom from arbitrary arrest and detention by imposing and increasing penalties of imprisonment and by allowing the arrest and remand of persons in custody pending consent of the Attorney-General for the prosecution of certain offences.

Penalties of imprisonment

47. The Bill limits the right to liberty by significantly increasing the penalty of imprisonment for the offences of espionage, sabotage and secrecy. The purpose of increasing the penalty of imprisonment for these offences is to ensure that the penalties reflect the gravity of each offence, particularly where the offence has been amended to include conduct which is more serious in nature. In this respect, the measures will address the growing risk that espionage and related activities pose to Australia's national security. Increasing penalties of imprisonment in these circumstances is consistent with the established principle of Commonwealth criminal law policy as set out in *the Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* (Guide to Framing Commonwealth Offences) to impose a heavier penalty where the consequences of the offence are particularly dangerous or damaging. Increasing penalties of imprisonment will also ensure effective deterrence of the commission of offences. A lack of serious criminal penalties for existing offences has resulted in a permissive operating environment for malicious foreign actors.

48. The Bill also limits the right to liberty by imposing a penalty of imprisonment for the new offences of foreign interference and theft of trade secrets. The penalty of 25 years for foreign interference, and 15 years for theft of the trade secrets, reflects an appropriate gradation with the amended penalties for treason, espionage, sabotage and secrecy which range from two years to life imprisonment. Consequently, the penalties for the new offences are proportionate and reflect the seriousness of the conduct engaged in. Tiered penalties for espionage, secrecy and foreign interference offences further ensure that penalties are commensurate with the seriousness and culpability of offending. The higher penalty in each of the tiered offences ensures that penalties are proportionate to the person's intent or the harm flowing from the offence.

49. The Bill further introduces an aggravated offence for providing false or misleading information in relation to an Australian Government security clearance. The aggravated offence will attract a maximum penalty of five years imprisonment as opposed to a maximum penalty of 12 months imprisonment for the underlying offence. The aggravated offence relates to providing false or misleading information in relation to an application for or the maintenance of, an Australian Government security clearance. The introduction of an aggravated offence and higher penalty reflects the significant national security risks of the provision of false or misleading information in security clearance processes. Failing to disclose, or providing false or misleading statements concerning, links to foreign individuals, entities and governments may be considered particularly harmful as vetting and security agencies are unable to adequately assess the risks and vulnerabilities of foreign influence or

interference if that person is given access to a range of classified material and places, disclosure of or access to which may cause significant harm. The introduction of the aggravated offence is also consistent with the Guide to Framing Commonwealth Offences principle to impose a heavier penalty where the consequences of the offence are particularly dangerous or damaging.

50. Responsibility for determining criminal guilt and imposing an appropriate sentence rests with the courts in their exercise of judicial power. The court will have discretion to implement an appropriate penalty based on all of the circumstances of the case. In this regard, the application of the penalties is not disproportionate. The offences will be subject to a number of safeguards to ensure their appropriate application and which promote the right to liberty and freedom from arbitrary detention including the availability of defences, bail and parole entitlements and fair trial rights such as to have matters heard by a competent, independent and impartial tribunal established by law.

Defences

51. Specific defences will be available for the offences of sabotage, espionage, foreign interference and secrecy. In addition to specific defences, the general defences under Part 2.3 of the Criminal Code will be available for all offences. These general defences include mistake or ignorance of fact, ignorance of subordinate legislation that was not available, claim of right over property, duress, sudden or extraordinary emergency, self-defence, and lawful authority. Defences will allow persons at risk of deprivations of liberty to justify their actions and defend the criminal charge against them.

Bail

52. Section 68 of the *Judiciary Act 1903* confers federal jurisdiction on state and territory courts for criminal matters including in relation to the procedure for and determination of bail for persons remanded in custody accused of a federal offence. As such, bail applications for federal offences are dealt with according to the bail procedure of the state or territory where the offence was committed. In most states and territories criminal procedure laws provide for a general presumption in favour of bail. This presumption ensures deprivations of liberty are kept to a minimum by allowing the temporary release of an accused pending criminal proceedings.

53. The general presumption in favour of bail may be displaced in certain circumstances. For example, it may be necessary to refuse bail to prevent the communication of information already within the knowledge or possession of the accused or to prevent interference with evidence or flight of the accused. The general presumption may also be displaced by a presumption against bail for certain offences. Under existing section 15AA of the Crimes Act, and the amendments in this Bill, bail must not be granted for offences including treason, treachery and espionage unless 'exceptional circumstances' apply. The presumption against bail is appropriately reserved for serious offences recognising the need to balance the right to liberty and the protection of the community.

54. For offences subject to a presumption against bail the accused will nevertheless be afforded to opportunity to rebut the presumption. Further, the granting or refusing of bail is not arbitrary, as it is determined by a court in accordance with the relevant rules and principles of criminal procedure.

Parole and early release

55. Under section 19AB of the Crimes Act, persons convicted of a federal offence will be entitled to parole in circumstances in which the court imposes a life sentence or an aggregate of sentences which exceeds three years and where the person is not already serving or subject to a federal sentence. The entitlement of parole will ensure that persons will be released from prison after serving a specified period of their federal sentence subject to conditions that they must obey while they are in the community.

56. As a further safeguard, persons serving a federal sentence may be entitled to early release on licence. Early release on licence allows the Attorney-General to consider exceptional circumstances in which a person should be released from prison prior to the expiration of their sentence. In deciding whether to grant a licence the Attorney-General may have regard to extensive cooperation by the person with law enforcement agencies before or after sentencing or any serious medical condition the person has that cannot adequately be treated or managed within the prison system.

57. The availability of parole and early release will ensure that lawful deprivations of liberty are no longer than is necessary in the circumstances.

Fair trial rights and minimum guarantees in criminal proceedings

58. Fair trial rights include the right to equality before courts and tribunals and the right to a fair and public hearing before a competence, independent and impartial court or tribunal established by law. Fair trial rights are supplemented by minimum guarantees in criminal proceedings which include to be tried in person and without undue delay, to be free from self-incrimination, to have a conviction and sentence reviewed by a higher court and not to be tried or punished for the same offence more than once. These rights and guarantees are protected in common law as well as in the Crimes Act, the *Evidence Act 1995* and in the criminal laws and procedures of states and territories.

59. Imprisonment following an unfair trial may amount to arbitrary detention. In these circumstances, the protection of fair trial rights and minimum guarantees will ensure the appropriate application of offences under the Bill and thereby protect the right to liberty and freedom from arbitrary detention.

60. On this basis, the limitation imposed on the right to liberty and freedom from arbitrary detention is reasonable, necessary and proportionate to achieving the legitimate objective of strengthening espionage and foreign interference laws to ensure the protection of Australians and Australia's national security.

Consent of the Attorney-General for prosecution

61. Under the Bill, the consent of the Attorney-General is required for the prosecution of an offence of espionage, foreign interference, sabotage, theft of trade secrets, or threats against security offences. The Bill confirms that the requirement for the Attorney-General to provide consent prior to proceedings being commenced for the commitment of a person for trial for an offence does not preclude the arrest, charge, remanding or releasing on bail of a person in relation to the offences. The arrest, charge and remand in custody of a person in such circumstances may limit the right to liberty and freedom from arbitrary arrest and detention, since the person arrested and detained would have no case to answer should the

Attorney-General decline to consent to a prosecution. The remand in custody of a person awaiting consent of the Attorney-General may also limit the right to be tried within a reasonable period or to be released.

62. The remand in custody of an accused may be necessary in the circumstances to prevent the communication of information already within the knowledge or possession of the accused which has the potential to damage Australian interests or otherwise threaten Australia's national security. It may also be necessary to prevent interference with evidence or flight of the accused. The granting or refusal of bail is not arbitrary, as it is determined by a court in accordance with the relevant rules and principles of criminal procedure. Further, the Bill ensures that nothing in the relevant provisions authorising arrest, charge, remand or release prior to the Attorney-General's consent will prevent the discharging of the accused if proceedings are not continued within a reasonable time. As such, if there is a significant delay between a person's arrest, charge, remand or release, and the decision of the Attorney-General, a person may be discharged and released from detention.

63. On this basis, the limitation imposed on the right to liberty and freedom from arbitrary detention is reasonable, necessary and proportionate to ensure the protection of Australia's national security.

Right to be tried without undue delay

64. Article 14(3)(c) of the ICCPR states that in the determination of any criminal charge, everyone has the right to be tried without undue delay. This right reflects the common law principle that 'justice delayed is justice denied'. It relates not only to the time by which a trial should commence, but also to the time by which it should conclude and judgment be given.

65. The right to be tried without undue delay may be limited where the delay is not 'undue' and where it is reasonable, necessary and proportionate to achieve a legitimate objective. According the Human Rights Committee, whether a delay is 'undue' will depend on the circumstances of each case taking into account the complexity and seriousness of the case and whether the accused is remanded in custody.

66. The Bill engages the right to be tried without undue delay by requiring consent of the Attorney-General for the prosecution of certain offences. The Bill limits the right to be tried without undue delay to the extent that a person may be charged, arrested and remanded in custody or on bail prior to and pending the Attorney-General's consent. The arrest, charge and remand in custody or on bail of an accused may be necessary in the circumstances to prevent the communication of information already within the knowledge or possession of the accused which has the potential to damage Australian interests or otherwise threaten Australia's national security. Further, the Bill ensures that nothing in the relevant provisions authorising arrest, charge, remand or release prior to the Attorney-General's consent will prevent the discharging of the accused if proceedings are not continued within a reasonable time. As such, if there is a significant delay between a person's arrest, charge, remand or release, and the decision of the Attorney-General, a person may be discharged.

67. On this basis, the limitation imposed on the right to be tried without undue delay is reasonable, necessary and proportionate to ensure the protection of Australia's national security.

Presumption of innocence

68. Article 14(2) of the ICCPR provides that everyone charged with a criminal offence shall have the right to be presumed innocent until proven guilty according to law. In General Comment No. 32 (CCPR/C/GC/32) the Human Rights Committee stated that the presumption of innocence imposes on the prosecution the burden of proving the charge and guarantees that no guilt can be presumed until the charge has been proved beyond reasonable doubt. The presumption of innocence may be limited provided the limitation 'is reasonable in the circumstances' and necessary and proportionate to achieve a legitimate objective.

69. The Bill limits the presumption of innocence by:

- imposing strict liability and absolute liability for certain offence elements
- placing an evidentiary burden on the defendant with respect to defences
- providing for evidentiary certificates which are prime facie evidence as to the existence of certain facts.

Strict liability

70. Strict liability applies to elements of the offences of espionage, secrecy and treason. For espionage offences these elements include that the information or thing dealt with has a security classification.

71. For secrecy offences strict liability applies to the element that the information disclosed or communicated is inherently harmful information to the extent that the information is security classified information. For aggravated espionage and secrecy offences the element that a person dealt with five or more documents or things each of which has a security classification is also subject to strict liability. Finally, for the offence of treason (assisting an enemy to engage in armed conflict) strict liability applies to the elements that the enemy is engaged in armed conflict against the Commonwealth or the Australian Defence Force and that the enemy is identified in a Proclamation made under section 80.1AB of the Criminal Code.

72. Strict liability also applies to elements of the advocating mutiny and treason offences to remove the requirement to prove that a body corporate knows that it is incorporated in Australia.

73. The effect of applying strict liability to an element of an offence is that no fault element needs to be proved. This means that the prosecution will be required to prove, for the offence of espionage for example; that information dealt with has a security classification but will not need to prove that the person who dealt with the information knew this. The application of strict liability may limit the presumption of innocence to the extent that it allows for the imposition of criminal liability without requiring the prosecution to prove fault in the defendant for that particular element. Strict liability provisions will not violate the presumption of innocence so long as they are reasonable in the circumstances, and maintain rights of defence.

74. For the elements relevant to information or articles carrying a security classification, this is appropriate because such information or articles are clearly marked with the security

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

75. In the case of the treason offence, it is not necessary for the person to have a state of mind as to the specific nature of a Proclamation made under section 80.1AB. The prosecution is already required to prove that the person was reckless as to whether the enemy was engaged in armed conflict involving the Commonwealth or the Australian Defence Force under paragraph 80.1AA(1)(a). It would be inappropriate for a prosecution to be able to proceed where a defendant knew a party was an enemy of Australia but was not aware of a substantial risk that there was a Proclamation made under section 80.1AB. The purpose of the Proclamation is to ensure that a person can identify whether there are any 'enemies' for the purpose of the treason offences should they wish to check, not for them to be specifically aware of the Proclamation in order to commit the offence.

76. The application of strict liability is also necessary to ensure that a person cannot avoid criminal responsibility because they were unaware of certain circumstances for example that information was security classified information. Consistent with the Guide to Framing Commonwealth Offences, requiring knowledge of such an element in these circumstances would undermine deterrence of the offence. There are also legitimate grounds for penalising a person's lacking 'fault' in these circumstances because, with an offence of espionage for example, the person still engaged in conduct with the intention to, or reckless as to whether, that conduct would prejudice Australia's national security or advantage the national security of a foreign country.

77. The application of strict liability will also make available the general defence of mistake of fact as set out in section 9.2 of the Criminal Code. This defence provides that a person is not criminally responsible for an offence that includes a physical element to which strict liability applies if:

- at or before the time of the conduct constituting the physical element, the person considered whether or not a fact existed, and is under a mistaken but reasonable belief about those facts, and
- had those facts existed, the conduct would not have constituted an offence.

78. The strict liability measures are proportionate in that they only apply to elements of the offence and not to the offences as a whole. In this respect, the prosecution will still be required to prove, beyond a reasonable doubt, all other elements of the offence including the fault elements of intention or recklessness.

Absolute liability

79. Absolute liability applies to a number of elements of the offences in the Bill.

80. Absolute liability also applies to jurisdictional elements of the offences. A jurisdictional element is an element of an offence that does not relate to the substance of the offence, but marks a jurisdictional boundary between matters that fall within the legislative power of the Commonwealth and those that do not. According to the Guide to Framing Commonwealth Offences, absolute liability should apply to all jurisdictional elements.

81. For example, the definition of 'public infrastructure' for the purpose of the sabotage offences applies absolute liability to the element that the infrastructure, facility, premises, network or electronic system 'belongs' to the Commonwealth and to the element that 'the infrastructure, facility, premises, network or electronic system belongs to, or is operated by, a constitutional corporation or used to facilitate constitutional trade or commerce'. These matters are not relevant to the offender's culpability and are included in order to link the offences to the Commonwealth's power to legislate under the Constitution.

82. As with strict liability, the application of absolute liability limits the presumption of innocence to the extent that it allows for the imposition of criminal liability without requiring the prosecution to prove fault in the defendant.

83. The application of absolute liability is also necessary to ensure that a person cannot avoid criminal responsibility because they were unaware of certain circumstances for example that property they damaged or destroyed belonged to a Commonwealth entity or of the level of government law that gave rise to a particular Australian democratic or political right. Consistent with the Guide to Framing Commonwealth Offences, requiring knowledge of such elements in these circumstances would undermine deterrence of the offences. There are also legitimate grounds for penalising a person's lacking 'fault' in these circumstances for example, because the person still intentionally damaged property or used violence to interfere with a person's political right or duty.

84. Further, the absolute liability measures are proportionate in that they only apply to elements of the offence and not to the offences as a whole. In this respect, the prosecution will still be required to prove, beyond a reasonable doubt, all other elements of the offence including fault elements of intention, knowledge or recklessness.

Reversal of burden of proof

85. The Bill creates a number of specific defences applying to the offences in the Bill, which reverse the burden of proof by providing that a defendant bears the evidential burden in proving the elements of the defence. Consistent with section 13.3 of the Criminal Code, this burden requires the defendant adduce or point to evidence that suggests a reasonable possibility that a particularly matter exists or does not exist. Reversing the burden of proof limits Article 14(2) in that a defendant's failure to discharge the burden may permit their conviction despite reasonable doubt as to their guilt.

86. It is reasonable and necessary for the burden of proof to be placed on the defendant where the facts in relation to the defence are peculiarly within the knowledge of the defendant. For example, for a defence at section 91.4(2) (espionage) a defendant should be readily able to point to evidence that they acquired the relevant information or article indirectly from a publically available source. For a defence at subsection 83.3(2) (military-style training involving foreign government principal) the defendant is best placed to know of the existence of the type of agreement therein and to provide evidence in relation to that agreement. Similarly, for a defence at section 80.3 the defendant is best placed to explain their motivations when engaging in the relevant conduct as it is peculiarly within their knowledge as to how and why they should be considered to be acting in good faith.

87. Reversal of proof provisions are proportionate because, as the prosecution will still be required to prove each element of the offence beyond reasonable doubt. Further, if the

defendant discharges an evidential burden, the prosecution will also be required to disprove those matters beyond reasonable doubt, consistent with section 13.1 of the Criminal Code.

Evidentiary certificates

88. Sections 93.3 and 121.3 of the Bill provide that a certificate signed by the Attorney-General is prima facie evidence that the information or thing specified in the certificate concerns Australia's national security or relates to security classified information. Evidentiary certificate provisions may limit Article 14(2) to the extent that they create a presumption as to the existence of the factual basis on which a certificate is issued which requires the accused to disprove the matters certified in the certificate. Accordingly, evidentiary certificate provisions reverse the burden of proof.

89. The evidentiary certificates provided for in the Bill will be used to settle formal matters of fact, being that certain information concerns national security or is security classified, which would otherwise be difficult to prove under the normal rules of evidence. This is because matters relating to national security and security classified information can be said to be peculiarly within the knowledge of the Commonwealth. By precluding a requirement on the prosecution to prove certain factual matters, the Bill will ensure that the accused is tried without delay in accordance with Article 14(3)(c) of the ICCPR. Furthermore, the evidentiary certificates will establish prima facie evidence, rather than conclusive evidence and as such may be challenged by the accused during the court proceedings. Importantly, the evidentiary certificates will not establish the weight or veracity of the evidence, which will remain a matter for the court.

90. On this basis, the limitations on the right to the presumption of innocence are reasonable, necessary and proportionate to achieving the legitimate objective of protecting Australia's national security.

Right to privacy

91. Article 17 of the ICCPR states that no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. The Human Rights Committee have interpreted the right to privacy as comprising freedom from unwarranted and unreasonable intrusions into activities that society recognises as falling within the sphere of individual autonomy. The right to privacy may be limited where the limitation is lawful and not arbitrary and where it is reasonable, necessary and proportionate to achieve a legitimate objective. The Bill limits the right to privacy in that it will enable the interception of telecommunications under the TIA Act in respect of the offences provided for in the Bill.

92. The gravity of the threat posed to Australia's national security by espionage, foreign interference and related activities demonstrates the need to take reasonable steps to detect, investigate and prosecute those suspected of engaging in such conduct. The current lack of law enforcement and intelligence powers with respect to these activities has resulted in a permissive operating environment for malicious foreign actors, which Australian agencies are unable to effectively disrupt and mitigate.

93. The interception regime is clearly authorised by law and its application authorised by the legislative framework in the TIA Act. Before issuing an interception warrant, the relevant authority must be satisfied that the agency is investigating a serious offence, the gravity of the

offence warrants intrusion into privacy and the interception is likely to support the investigation. This threshold acts as a safeguard against the arbitrary or capricious use of the interception regime and also ensures that any interception will be proportionate to the national security objective.

94. Moreover, there is independent oversight of the use of interception powers of law enforcement agencies by the Commonwealth Ombudsman. At least twice a year, the Commonwealth Ombudsman must inspect bodies such as the AFP in relation to their use, dissemination and destruction of intercepted information. The Commonwealth Ombudsman is also required under the TIA Act to report to the Attorney-General about these inspections, including any information about deficiencies identified and remedial action.

95. The safeguards identified and the legal framework around which interception warrants are issued ensure that the use of this power is prescribed by law and not arbitrary. Accordingly, the limitation on the right to privacy is reasonable, necessary and proportionate to achieve the legitimate objective of assisting of ensuring the protection of Australia's national security.

Freedom of expression

96. Article 19(2) of the ICCPR states that everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice. Any limitation on the right to freedom of expression must be reasonable, necessary, and proportionate for the pursuit of a legitimate objective and for the respect of the rights or reputations of others or for the protection of national security, public order, or public health or morals.

97. The Bill engages the right to freedom of expression by:

- replacing the offence of 'inciting mutiny' with the offence of 'advocating mutiny', and
- amending secrecy offences to better deal with unauthorised disclosure and unlawful handling of Commonwealth information.

Advocating mutiny

98. The new offence of advocating mutiny will apply where a person advocates mutiny, reckless as to whether the result will be that a member of the defence force takes part in a mutiny. The term 'mutiny' will be defined as a combination between persons who are, or at least 2 of whom are, members of the Australian Defence Force (ADF) who overthrow lawful authority in the ADF or in a force of another country that is acting in cooperation with the ADF; or who resist such lawful authority in such a manner as to substantially prejudice the operational efficiency of the ADF or of, or of a part of, a force of another country that is acting in cooperation with the ADF. The term 'advocating' is intended to take its ordinary meaning and could include supporting, recommending, promoting, encouraging, urging and inciting. Such conduct falls within the scope of the right to freedom of expression in so far as advocating is form of expression which involves the imparting of information and ideas. By criminalising conduct which advocates mutiny, the Bill will limit the right to freedom of expression.

99. As established, the criminalisation of conduct which advocates mutiny will ensure the protection of the prohibitions contained in Article 20 regarding propaganda for war and advocacy of national, racial or religious hatred. According to the Human Rights Committee, the prohibitions provided for in Article 20 are fully compatible with the right to freedom of expression, the exercise of which carries special duties and responsibilities. As such, according to the Committee, any limitation that is justified on the basis of Article 20 must still comply with Article 19(3), that is that it must be necessary for the respect of the rights or reputations of others or for the protection of national security, public order, or public health or morals.

100. The primary responsibility of the Australian Defence Force is to defend Australia and Australia's interests. By seeking to overthrow the defence force of Australia, acts of mutiny clearly threaten Australia's national security and public order. In certain circumstances, acts of mutiny may also result in the arbitrary detention, torture or cruel, inhuman or degrading treatment or even the death of persons. Prohibiting conduct which advocates mutiny in these circumstances will promote the rights of others including the right to life, the right to liberty and the right not to be subject to torture as covered by Article 6, 7 and 9 of the ICCPR respectively. The gravity of the threat posed by acts of mutiny both to Australia's national security and public order and to the rights and freedoms of others demonstrates the need to take reasonable steps to discourage behaviour that promotes such activities. Besides prohibition there is no less restrictive measure to ensure the deterrence of conduct which advocates mutiny. The availability of the general defences under Part 2.3 of the Criminal Code including the defences of duress and self-defence will ensure that the application of the offence of advocating mutiny is reasonable and proportionate to achieve its objective.

Secrecy

101. Secrecy offences relating to inherently harmful information will apply where a person communicates or publishes (subsection 122.1(1)) or otherwise deals with (subsection 122.1(2)) inherently harmful information and the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity. Secrecy offences causing harm to Australia's interests will apply where a person communicates (subsection 122.2(1)) or otherwise deals with (subsection 122.1(2)) information, the communication or dealing with causes, will cause or is likely to cause harm to Australia's interest and the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity. A person deals with information if the person receives, obtains, collects, possesses, makes a record of, copies, alters, conceals, communicates, publishes or makes available the information. Further, an offence of unauthorised disclosure of information (section 122.4) will apply where a person communications information which was made or obtained by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity; and the person is under a duty, which rises under law of the Commonwealth, not to disclose the information.

102. Conduct which receives, obtains, collects, communicates, publishes or makes available information clearly falls within the scope of the right to freedom of expression in so far as it involves the seeking, receiving or imparting of information and ideas. By criminalising these activities in certain circumstances secrecy offences will limit the right to freedom of expression.

103. In General Comment No. 34 (CCPR/C/GC/34) the Human Rights Committee stated that care must be taken by States parties to ensure official secrets laws, are crafted and applied in a manner that conforms to the requirements of Article 19(3). According to the Committee:

> It is not compatible with paragraph 3, for instance, to invoke such laws to suppress or withhold from the public information of legitimate public interest that does not harm national security or to prosecute journalists, researchers, environmental activists, human rights defenders, or others, for having disseminated such information. Nor is it generally appropriate to include in the remit of such laws such categories of information as those relating to the commercial sector, banking and scientific progress.

104. The offences in section 122.1 apply only to information within narrowly defined categories of inherently harmful information. The offences in section 122.2 apply only to information made or obtained by a Commonwealth officer, the communication of which would cause harm to specified essential public interests, and where that harm does or was likely to eventuate as a result of the person's conduct. The gravity of the threat posed by the disclosure of inherently harmful information or information which causes or will cause harm to Australia's interests demonstrates the need to criminalise such conduct.

105. Section 122.4 does not criminalise the disclosure of any particular information in its own right. Section 122.4 contains a narrower and modernised version of the general secrecy offence currently contained in section 70 of the Crimes Act, which will make it an offence for a Commonwealth officer or a person engaged to perform work for a Commonwealth entity to communicate information in breach of a duty arising elsewhere under the law of the Commonwealth. As such, section 122.4 does not establish a new limitation on the ability of such persons to communicate information.

106. The availability of the general defences under Part 2.3 of the Criminal Code as well as the specific defences provided for in section 122.5 will further ensure that the application of secrecy offences is reasonable and proportionate to achieve their objective

Freedom of assembly and association

107. Article 21 of the ICCPR recognises the right to peaceful assembly. This right protects the rights of individuals and groups to meet and to engage in peaceful protest. Article 21 extends to all gatherings for peaceful purposes, regardless of the degree of public support for the purpose of the gathering. Article 22 of the ICCPR states that everyone shall have the right to freedom of association with others. This right protects the right to form and join associations to pursue common goals.

108. The Bill engages the right to freedom of assembly and association by replacing the offence of 'unlawful drilling' with the offence of 'military-style training involving a foreign government principal'. This offence applies where a person provides, receives or participates in training that involves using arms or practising military exercises, movements or evolutions on behalf of or directed, funded or supervised by a foreign government principal or by a person acting on behalf of a foreign government principal.

109. The conduct involved in the offences falls within the scope of Articles 21 and 22 to the extent that the meeting of one or more persons for the purpose of military-style training

constitutes an assembly and/or an association of persons. By criminalising such conduct, the Bill will limit the right to freedom of assembly and association. Any limitation on the freedom of assembly and association must be necessary in a democratic society in the interest of national security or public safety, public order, the protection of health or morals or the protection of the rights and freedoms of others.

110. Military-style training on behalf of a foreign government can erode Australia's sovereignty and undermine the authority of the Australian military. On this basis, military-style training threatens Australia's national security and public order. In the worst case scenario, military-style training may result in the death of persons. Prohibiting military-style training in these circumstances will promote public safety and the rights of others including the right to life as covered by Article 6 of the ICCPR.

111. The gravity of the threat posed by military-style training both to Australia's national security, public safety and public order and to the rights of others demonstrates the need to take reasonable steps to prevent such activities. Besides prohibition there is no less restrictive measure to ensure the deterrence of military-style training. The availability of the general defences under Part 2.3 of the Criminal Code and the specific defences provided in section 83.3 ensures that the application of the offence is reasonable and proportionate to achieve its objective.

Conclusion

112. The Bill is compatible with human rights because it promotes the protection of a number of human rights including the right to liberty, the right to freedom expression, assembly and association and the right to take part in public affairs and elections. To the extent that it may limit human rights, those limitations are reasonable, necessary and proportionate to the legitimate objective of the Bill, that is primarily to ensure the protection of Australia's national security.

NOTES ON CLAUSES

Preliminary

Clause 1 – Short title

113. This clause provides that when the Bill is enacted, it is to be cited as the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2017*.

Clause 2 – Commencement

114. This clause sets out when the various parts of the Act are to commence.

115. Item 1 of the table provides that sections 1 to 3 and anything else in the Act not elsewhere covered by the table in Clause 2 commence the day the Act receives Royal Assent.

116. Item 2 of the table provides that Schedule 1 (Treason, espionage, foreign interference and related offences) commences the day after the Act receives Royal Assent.

117. Item 3 of the table provides that Schedule 2 (Secrecy) commences on a single day to be fixed by Proclamation. However, if the provisions do not commence within the period of six months beginning on the day the Act receives Royal Assent, they commence on the day after the end of that period. Commencement by Proclamation is appropriate to ensure appropriate regulations can be made to support key definitions in Schedule 2 and to ensure that departments and agencies can provide appropriate information to staff and contractors about the new offences.

118. Item 4 of the table provides that Schedule 3 (Aggravated offence for giving false or misleading information) commences the day after the Act receives Royal Assent.

119. Item 5 of the table provides that Part 1 of Schedule 4 (Telecommunications serious offences) commences the day after the Act receives Royal Assent.

120. Item 6 of the table provides that Part 2 of Schedule 4 (Telecommunications serious offences) commences at the same time as Schedule 2 (covered by Item 3 of the table).

121. Item 7 of the table provides that Schedule 5, Part 1 commences at the same time as the *Foreign Influence Transparency Scheme Act 2017* commences. If the *Foreign Influence Transparency Scheme Act 2017* does not commence, then Part 1 of Schedule 5 will not commence at all.

122. 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*.

123. However, if both of the events listed above do not occur then Part 2 of Schedule 5 will not commence at all.

Clause 3 – Schedules

124. This is a formal clause that enables the Schedules to amend Acts by including amendments under the title of the relevant Act.

SCHEDULE 1 - TREASON, ESPIONAGE, FOREIGN INTERFERENCE AND RELATED OFFENCES

General Outline

125. The purpose of Schedule 1 is to make amendments to offences relevant to Australia's defence and security. The amendments will ensure Commonwealth law comprehensively criminalises activities that could prejudice Australia's national security or facilitate the intelligence activities of foreign governments.

126. The amendments in Schedule 1 will send an important deterrence message to Australia's foreign adversaries that conduct that prejudices Australia's national security will not be tolerated.

Espionage

127. The Criminal Code currently contains espionage offences, but these are too narrow and have not evolved to deal with the modern threat environment.

128. Schedule 1 amends Part 5.2 of the Criminal Code to introduce comprehensive new espionage offences in Division 91. The new offences criminalise a broad range of dealings with information, including possessing or receiving, and protect a broader range of information, including unclassified material. The current methodology of Australia's adversaries means that dealings with unclassified information, if accompanied by the requisite intention to harm Australia, can be as damaging as the passage of classified information. The new offences will not just target the person who discloses the information, but also the actions of the foreign principal who receives the information. The new offences in Division 91 will also, for the first time, criminalise soliciting or procuring a person to engage in espionage and will introduce a new preparation or planning offence, which will allow law enforcement agencies to intervene at an earlier stage to prevent harmful conduct occurring.

Foreign interference

129. Currently, Commonwealth criminal law contains no offences targeting conduct undertaken by foreign government that falls short of espionage but is intended to harm Australia's national security or influence Australia's political or governmental processes.

130. Schedule 1 introduces new Division 92 into Part 5.2 of the Criminal Code which will contain new foreign interference offences. These offences complement the espionage offences by criminalising a range of other harmful conduct undertaken by foreign principals who seek to interfere with Australia's political, governmental or democratic processes, to support their own intelligence activities or to otherwise prejudice Australia's national security. The offences will apply where a person's conduct is covert or deceptive, involves threats or menaces or does not disclose the fact that conduct is undertaken on behalf of a foreign principal. New Division 92 also criminalises the provision of support or funding to foreign intelligence agencies.

Sabotage

131. The Commonwealth's current sabotage offence was introduced into the Crimes Act in 1960 and has not evolved to reflect the modern threat environment. The existing sabotage

offence only protects Defence facilities. Schedule 1 introduces comprehensive sabotage offences into new Division 82 in Part 5.1 of the Criminal Code. The new sabotage offences will criminalise conduct causing damage to a broad range of critical infrastructure where it could prejudice Australia's national security. The offences in new Division 82 will apply higher penalties where sabotage offences are committed on behalf of foreign principals. New Division 82 will also contain offences that apply where a person's conduct does not immediately cause damage, but leaves an item or system vulnerable to future misuse or exploitation.

Theft of trade secrets on behalf of a foreign government

132. Schedule 1 introduces a new offence targeting theft of trade secrets on behalf of a foreign government. This amounts to economic espionage and can severely damage Australia's national security and economic interests. The new offence will apply to dishonest dealings with trade secrets on behalf of a foreign actor.

Treason and other threats to security

133. Although rarely used, treason offences are a critical part of Commonwealth criminal law. Part II of the Crimes Act also contains a series of rarely used offences protecting the security and defence of the Commonwealth. These offences require modernisation to reflect the modern environment.

134. Schedule 1 amends Part 5.1 of the Criminal Code to modernise Australia's treason offences. It will ensure that treason offences regarding assisting an enemy to engage in armed conflict against Australia, which carries a penalty of life imprisonment, appropriately reflect moderns terminology related to armed conflict. The amendments to Part 5.1 will also create a new offence of treachery in the Criminal Code (replacing the existing archaic and antiquated treachery offence in section 24AA of the Crimes Act) that applies where a person seeks to use force or violence to overthrow the Constitution or an Australian government.

135. Schedule 1 introduces new Division 83 into Part 5.1 of the Criminal Code. Division 83 will modernise and improve the existing offences against government in Part II of the Crimes Act (which will be repealed). The offences in Division 83 aim to protect Australia's defence by criminalising advocating mutiny, assisting prisoners of war to escape and military-style training by foreign governments. New Division 83 also criminalises interference with Australian democratic or political rights where the conduct involves the use of force, violence or intimidation.

PART 1 – MAIN AMENDMENTS

Criminal Code Act 1995

Item 1

136. Item 1 repeals the heading of Part 5.1 of the Criminal Code and substitutes a new heading. The heading is changing from 'Treason, urging violence and advocating terrorism or genocide' to 'Treason and related offences'. The heading requires updating to reflect the broader range of offences within Part 5.1 due to the enactment of new sabotage offences in Division 82 and new offences dealing with other threats to security in new Division 83following the repeal of Part II of the Crimes Act (by Item 43 of Schedule 1).

Item 2

137. Item 2 repeals the heading of section 80.1A of the Criminal Code and substitutes a new heading. The heading is changing from 'Definition of *organisation*' to 'Definitions'. This change is needed because an additional definition is being added to section 80.1A by Item 3.

Item 3

138. Item 3 inserts a new definition of ***party*** in section 80.1A of the Criminal Code. This term is used in the new treason offence in section 80.1AA (to be inserted by Item 4) and is defined to include a person, body or group of any kind. This is intended to reflect the broad range of organisations or groups who may engage in armed conflict with the Commonwealth or the Australian Defence Force. This will range from nation states through to organised armed groups using force to achieve their purposes. An example of an organised armed group would be a separatist or rebel group seeking to overthrow the government of another nation state.

Item 4

Section 80.1AA – Treason – assisting enemy to engage in armed conflict

139. Item 4 repeals existing section 80.1AA, which contains two offences of 'Assisting enemies at war with the Commonwealth' (at subsection 80.1AA(1)) and 'Assisting countries etc. engaged in armed hostilities against the ADF' (at subsection 80.1AA(4)).

140. Item 4 combines the existing offences in subsections 80.1AA(1) and (4) into one new offence titled 'Treason – assisting enemy to engage in armed conflict'. This new offence simplifies the structure of the treason offences, updates the references in the offence to reflect modern international terminology about armed conflict and removes the confusing terminology at existing subsection 80.1AA(4) about 'armed hostilities'. The new offence carries a maximum penalty of life imprisonment, which is consistent with the existing treason offences at subsections 80.1AA(1) and (4).

141. Consistent with the existing treason offences, this offence will only be able to be committed by a person who owes an allegiance to the Commonwealth (paragraph 80.1AA(1)(f)). The person must know that they owe an allegiance to the

Commonwealth. This is appropriate because only persons who benefit from the protection of the Australian nation state should be able to commit treason against Australia.

142. The offence will also only be able to be committed if the Commonwealth has, by proclamation made by the Governor-General, declared a party to be an enemy engaged in armed conflict involving the Commonwealth or the Australian Defence Force (paragraph 80.1AA(1)(a)), that is, if a party is the Commonwealth's adversary in armed conflict. A person should not be able to commit treason against Australia if it was impossible for them to know that another party was Australia's enemy. The requirement for the Commonwealth to proclaim its enemies for the purpose of the treason offence at section 80.1AA ensures that there is a publicly accessible record of enemies against whom the Commonwealth is engaged in an armed conflict for the purposes of the treason offence at section 80.1AA.

143. An example of this offence is as follows. Person A is a dual citizen of Australia and Country X, a repressive regime seeking to expand its territory. As part of a coalition of nation states, Australia has been engaged in an international armed conflict with Country X for two years (and the Governor-General has declared Country X to be an enemy for the purpose of section 80.1AA). Hostilities between Country X and the Australia are occurring primarily in the airspace above Country X's territorial sea. Person A still holds a strong connection to Country X and does not support Australia's military action. Person A has access to classified information about Royal Australian Air Force (RAAF) operations and passes details of a planned operation to a friend who works in the military forces of Country X. As a result, Country X uses anti-aircraft weapons to shoot down Australian aircraft, resulting in casualties to RAAF personnel and destroying Australia's aircraft, thereby enabling Country X to gain a military advantage over Australia.

144. To establish this offence, the prosecution will have to prove beyond a reasonable doubt that:

- a party (the enemy) was engaged in armed conflict involving the Commonwealth or the Australian Defence Force and the person was reckless as to this element
- the enemy was identified in a Proclamation made under section 80.1AB
- the person intentionally engaged in conduct
- 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 conduct materially assisted the enemy to engage in armed conflict involving the Commonwealth or the Australian Defence Force, and
- at the time he or she engaged in the conduct, the person was:
    - was an Australian citizen, and knew that he or she was an Australian citizen

- was a resident of Australia, and knew that he or she was an Australian citizen
- had voluntarily put him or herself under the protection of the Commonwealth, and knew that he or she had done so, or
- was a body corporate incorporated by or under a law of the Commonwealth or of a State or Territory.

145. Recklessness is the fault element for paragraph 80.1AA(1)(a). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and
- a result if he or she is 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 the risk.

146. Strict liability will apply to paragraph 80.1AA(1)(b) consistent with subsection 80.1AA(2).

147. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 80.1AA(1)(c). Intention also applies to paragraph 80.1AA(1)(d). Under subsection 5.2(1) of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

148. Absolute liability applies to paragraph 80.1AA consistent with subsection 80.1AA(3).

149. The fault element for subparagraphs 80.1AA(1)(f)(i) and (ii) is knowledge. Under section 5.3 of the Criminal Code, a person has knowledge of a circumstance if he or she is aware that it exists or that it will exist in the ordinary course of events.

150. Strict liability applies to paragraph 80.1AA(1)(f)(iii) due to the application of subsection 80.1AA(2).

151. For paragraph 80.1AA(1)(a) of the offence, the prosecution will have to prove beyond a reasonable doubt that a party (the 'enemy') is engaged in armed conflict involving the Commonwealth or the Australian Defence Force and that the person was reckless as to this element. The term ***party*** is defined in section 80.1A (as amended by Item 3) to include a person, body or group of any kind. The use of the term 'armed conflict' is intended to cover both international armed conflicts and non-international armed conflicts. The prosecution will also have to prove that the defendant was aware of a substantial risk that an enemy was engaged in armed conflict involving the Commonwealth or Australian Defence Force and that, having regard to the circumstances known to him or her, it was unjustifiable to take the risk.

152. For paragraph 80.1AA(1)(b) of the offence, the prosecution will have to prove beyond a reasonable doubt that the enemy is identified in a Proclamation made under section 80.1AB. Consistent with subsection 80.1AA(2), strict liability will apply to paragraph 80.1AA(1)(b). Strict liability is set out in section 6.1 of the Criminal Code. The effect of applying strict

liability to an element of an offence means that no fault element needs to be proved and the defence of mistake of fact is available.

153. Applying strict liability to this element of the offence is appropriate because it is not necessary for the person to have a state of mind as to the specific nature of a Proclamation made under section 80.1AB. The prosecution is already required to prove that the person was reckless as to whether the enemy was engaged in armed conflict involving the Commonwealth or the Australian Defence Force under paragraph 80.1AA(1)(a). It would be inappropriate for the defendant to be able to avoid criminal liability for the offence because they lacked specific knowledge of the Proclamation, especially because the prosecution is required to prove that the person was reckless as to whether their conduct would materially assist an enemy to engage in armed conflict involving the Commonwealth or the Australian Defence Force in paragraph 80.1AA(1)(a)). The purpose of the Proclamation is to ensure that a person can identify whether there are any 'enemies' for the purpose of the treason offences should they wish to check, not for them to be specifically aware of the Proclamation in order to commit the offence.

154. The defence of mistake of fact is set out in section 9.2 of the Criminal Code. The defence provides that a person is not criminally responsible for an offence that includes a physical element to which strict liability applies if:

- at or before the time of the conduct constituting the physical element, the person considered whether or not a fact existed, and is under a mistaken but reasonable belief about those facts, and

- had those facts existed, the conduct would not have constituted an offence.

155. This defence would be available if, for example, a defendant had specifically turned his or her mind to whether there was a Proclamation under section 80.1AB and had mistakenly, but reasonably, concluded that no such Proclamation existed.

156. The defendant bears an evidential burden in relation to this defence. Section 13.3 of the Criminal Code provides that in the case of a standard 'evidential burden' defence, the defendant bears the burden of pointing to evidence that suggests a reasonable possibility that the defence is made out. If this is done, the prosecution must refute the defence beyond reasonable doubt (section 13.1).

157. For paragraph 80.1AA(1)(c), the prosecution will have to prove beyond a reasonable doubt that the person intentionally engaged in conduct. Consistent with subsection 4.1(2) of the Criminal Code, the reference to 'engages in conduct' in paragraph 80.1AA(1)(c) means to do an act or to omit to perform an act.

158. 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.

159. For paragraph 80.1AA(1)(e), the prosecution must prove beyond a reasonable doubt that the person's conduct materially assisted the enemy to engage in armed conflict involving the Commonwealth or the Australian Defence Force. This result must occur for the offence in section80.1AA to be committed. Absolute liability applies to this element, consistent with subsection 80.1AA(3). Absolute liability is set out in section 6.2 of the Criminal Code. The effect of applying absolute liability to an element of an offence is that no fault element needs to be proved and the defence of mistake of fact is unavailable.

160. Absolute liability is appropriate for this element because the prosecution is already required to prove the person's intention to materially assist the enemy in paragraph 80.1AA(1)(d). The purpose of the element in paragraph 80.1AA(1)(e) is to require proof of the physical element that the person's conduct materially assisted the enemy to engage in armed conflict involving the Commonwealth or the Australian Defence Force.

161. If absolute liability did not apply then, consistent with section 5.6 of the Criminal Code, recklessness would be the fault element for paragraph 80.1AA(1)(e). It is unnecessary for the prosecution to prove the lower fault element of recklessness for paragraph 80.1AA(1)(e) when the prosecution will already have proved the higher fault element of intention for the same physical element in paragraph 80.1AA(1)(d).

162. For subparagraph 80.1AA(1)(f)(i) or (ii), the prosecution will have to prove beyond a reasonable that, at the time he or she engaged in the conduct, the person was, and knew that he or she was, :

- an Australian citizen (defined in section 2B of the Acts Interpretation Act and section 4 of the Australian Citizenship Act)
- a resident of Australia (defined in the Dictionary to the Criminal Code as an individual who is a resident of Australia), or
- voluntarily under the protection of the Commonwealth (for example through the grant of asylum).

163. Under section 5.3 of the Criminal Code, a person has knowledge of a circumstance if he or she is aware that it exists or that it will exist in the ordinary course of events.

164. For subparagraph 80.1AA(1)(f)(iii), the prosecution will have to prove that the person is a body corporate incorporated by or under a law of the Commonwealth or of a State or Territory. Strict liability is appropriate for this element because section 12.3 of the Criminal Code (which provides that where knowledge is a fault element, the element attributed to a body corporate is that they 'expressly, tacitly or impliedly authorised or permitted the commission of the offence') does not fit well with establishing that the body corporate 'knows' it is incorporated under a law of the Commonwealth. The defence of mistake of fact, set out in section 9.2 of the Criminal Code, will apply.

165. Paragraph 80.1AA(1)(f) ensures that a person only commits this offence if he or she knows that they owe an allegiance to the Commonwealth. This is appropriate because only persons who benefit from the protection of the Australian state should be able to commit treason against the Commonwealth.

166. The penalty for this offence is life imprisonment. This is appropriate because the offence, at its core, represents a violation or betrayal of a person's allegiance to Australia by providing assistance to an enemy in an armed conflict against which Australia is engaged in fighting. This is one of the most serious offences in Commonwealth criminal law and is deserving of the most serious penalty.

167. Note 1 under subsection 80.1AA(1) clarifies that the existing defence in section 80.3 for acts done in good faith is available in relation to the offence at subsection 80.1AA(1).

168. Note 2 under subsection 80.1AA(1) clarifies the effect of subsection 4B(3) of the Crimes Act. Subsection 4B(3) provides that, if a body corporate is convicted of an offence against subsection 80.1AA(1), a court may impose a fine of up to 10,000 penalty units.

169. Subsection 80.1AA(4) provides a defence to the offence at subsection 80.1AA(1) if a person engaged in conduct solely by way of, or for the purposes of, the provision of aid or assistance of a humanitarian nature. The provision of aid or assistance of a humanitarian nature would include activities that are humanitarian in character and are conducted by or in association with the International Committee of the Red Cross, the United Nations or its agencies, and agencies contracted or mandated to work with the UN or its agencies. This is consistent with the existing defence in subsection 80.1AA(6) and is intended to ensure that a person is not criminally liable for this offence if they provided material assistance to a party, for example by providing financial aid or food, but intended genuinely to engage in humanitarian activities instead of to support the party to engage in armed conflict against Australia.

170. The Note under the defence at subsection 80.1AA(4) clarifies that the defendant will bear an evidential burden in relation to this defence. Section 13.3 of the Criminal Code provides that in the case of a standard 'evidential burden' defence, the defendant bears the burden of pointing to evidence that suggests a reasonable possibility that the defence is made out. If this is done, the prosecution must refute the defence beyond reasonable doubt (section 13.1). This is appropriate because a person's intention in providing aid or assistance of a humanitarian nature is peculiarly within his or her knowledge. The person will need to point to evidence that suggests a reasonable possibility that the defence is made out, which could include the fact that the conduct was undertaken through the UN, ICRC, an agency contracted or mandated to work with the UN or its agencies or a legitimate, registered charity. If this is done, the prosecution must refute the defence beyond reasonable doubt (section 13.1).

<u>Section 80.1AB – Proclamation of enemy engaged in armed conflict</u>

171. Section 80.1AB empowers the Governor-General to, by Proclamation, declare a party identified in the Proclamation to be an enemy engaged in armed conflict involving the Commonwealth or the Australian Defence Force.

172. A person should not be able to commit treason against Australia if it was impossible for them to know that another party was an enemy of Australia or the Australian Defence Force. The requirement for the Commonwealth to proclaim its enemies for the purpose of the treason offence at section 80.1AA ensures that there is a publicly accessible record of enemies with whom the Commonwealth is engaged in armed conflict.

173. The Proclamation as described at section 80.1AB will be subject to Parliamentary scrutiny and will be publically accessible. In accordance with the *Legislation Act 2003*, unless exempt, declarations by legislative instrument can be disallowed by Parliament. In accordance with section 38 of the Legislation Act, disallowable instruments must be tabled in each House of Parliament within six days of the instrument being registered. If a legislative instrument is disallowed, then it is repealed and ceases to have effect.

174. A Note to section 80.1AB notifies the reader that the offence provision at subsection 80.1AA(1) deals with the effect of the Proclamation.

Section 80.1AC – Treachery

175. Section 80.1AC will replace the existing treachery offence at subsection 24AA(1) of the Crimes Act, which is repealed by Item 43 of Schedule 1. The new treachery offence will criminalise the use of force or violence intended to overthrow the Constitution, the Government of the Commonwealth or of a State or Territory or the lawful authority of the government of the Commonwealth. The new treachery offence will carry a penalty of life imprisonment.

176. The existing treachery offence at subsection 24AA(1) is not being replicated in the new treachery offence at section 80.1AC to the extent that it relates to acts intended to overthrow the government of a proclaimed country. These are more appropriately dealt with by the laws of the relevant country or through the foreign incursions offences in Part 5.5 of the Criminal Code.

177. The existing treachery offence at subsection 24AA(2) is not being replicated in the new treachery offence because assisting enemies of the Australian Defence Force is covered by the treason offence in section 80.1AA, as inserted by Item 4 of Schedule 1.

178. An example of the offence is as follows. Person B holds the strong view that Australia's constitutional democracy does not best serve the interests of the Australian people and that anarchy is preferable. Person B forms an anarchist group with a large number of like-minded people and they storm Parliament House. Using weapons and violence, the group seeks to cause harm to a large number of parliamentarians, intending that the anarchist movement will remove the established government.

179. This offence complements the existing treason offence at section 80.1 of the Criminal Code targeting conduct causing death or harm to the Sovereign, Governor-General or Prime Minister and the offence at section 80.2 of the Criminal Code regarding urging another person to overthrow, by force or violence, the Constitution, the Government of the Commonwealth or a State or Territory or the lawful authority of the Government of the Commonwealth.

180. To establish this offence, the prosecution will need to prove beyond a reasonable doubt that:

- the person intentionally engaged in conduct
- the conduct involves force or violence and the person was reckless as to this element

- the person engaged in the conduct with the intention of overthrowing:
    - the Constitution
    - the Government of the Commonwealth or of a State or Territory, or
    - the lawful authority of the government of the Commonwealth.

181. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 80.1AC(1)(a). Under subsection 5.2(1) of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

182. Recklessness is the fault element for paragraph 80.1AC(1)(b). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and
- a result if he or she is 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 the risk.

183. For paragraph 80.1AC(1)(a), the prosecution will have to prove beyond a reasonable doubt that the person intentionally engaged in conduct. Consistent with subsection 4.1(2) of the Criminal Code, the reference to 'engages in conduct' in paragraph 80.1AC(1)(a) means to do an act or to omit to perform an act.

184. For paragraph 80.1AC(1)(b), the prosecution will have to prove beyond a reasonable doubt that the person's conduct involved force or violence and that the person was reckless as to this element. Therefore, the defendant must have been aware of a substantial risk that his or conduct involved force or violence and, having regard to the circumstances known to him or her it was unjustifiable to take that risk. Consistent with the offences in Subdivision C of Division 80 of the Criminal Code, the term 'force or violence' is not defined and will have its ordinary meaning.

185. 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.

186. Whether or not the overthrow of the Constitution or government occurs or the conduct is capable of bringing it about is not relevant to the defendant's culpability for the offence. For example, Person B's conduct may not be capable of defeating the security measures in place at Parliament House and therefore Person B's conduct was not capable of overthrowing

the Government. The defendant could still commit the offence despite the fact that this outcome does not occur, or is not capable of occurring.

187. The offence at section 80.1AC will be punishable by a maximum penalty of life imprisonment. This is appropriate because of the serious threat to the stability and security of Australia caused by conduct involving force or violence that is intended to overthrow an Australian government or the Constitution. The penalty is also consistent with the existing penalty of life imprisonment for the treachery offence at section 24AA of the Crimes Act.

188. Note 1 under subsection 80.1AC(1) clarifies that the existing defence in section 80.3 for acts done in good faith is available in relation to the offence at subsection 80.1AC(1).

189. Note 2 under subsection 80.1AC(1) clarifies the effect of subsection 4B(3) of the Crimes Act. Subsection 4B(3) provides that, if a body corporate is convicted of an offence against subsection 80.1AC(1), a court may impose a fine of up to 10,000 penalty units.

Item 5

190. Item 5 amends subsection 80.3(1) of the Criminal Code to insert the words 'and section 83.4' after the words 'Subdivisions B and C'. The effect of this amendment is to apply the defence for acts done in good faith in section 80.3 to the new offence of 'Interference with political rights and duties' in new section 83.4.

Item 6

191. Item 6 repeals existing paragraphs 80.3(2)(b), (c), (d) and (e) of the Criminal Code and creates a new paragraph 80.3(2)(b) that reflects the language of the new treason offence at section 80.1AA.

192. Paragraph 80.3(2)(b) provides clarity about the matters the Court can have regard to when considering whether the defence of acts of good faith applies. Under new paragraph 80.3(2)(b), to be inserted by Item 6, the Court may have regard to any matter, including whether the acts constituting the offence were done with the intention of assisting an enemy:

- engaged in armed conflict involving the Commonwealth or the Australian Defence Force, and

- declared in a Proclamation made under section 80.1AB to be an enemy engaged in armed conflict involving the Commonwealth or the Australian Defence Force.

193. This amendment ensures that the matters the Court may take into account when considering the applicability of the defence at subsection 80.3(1) are consistent with the language of the new treason offence at section 80.1AA.

194. Item 6 repeals paragraphs 80.3(2)(c), (d) and (e) of the Criminal Code. This amendment is required to reflect the repeal of the existing offences at subsection 80.1AA(4) and section 24AA of the Crimes Act.

195. Existing paragraph 80.3(2)(c) provides that a Court may take into account whether a person's acts were done with the intention of assisting another country, or an organisation, that is engaged in armed hostilities against the Australian Defence Force. This reflects the elements of the existing offence of 'Assisting countries etc. engaged in armed hostilities against the ADF' in subsection 80.1AA(4), which is being repealed by Item 4 of Schedule 1.

196. Following the repeal of the offence at subsection 80.1AA(4), it will not be necessary for a Court to be able to take these matters into account when considering a defence under subsection 80.3(1).

197. Existing paragraph 80.3(2)(d) provides that a Court may take into account whether a person's acts were done with the intention of assisting a proclaimed enemy of a proclaimed country (within the meaning of subsection 24AA(4) of the Crimes Act). Existing paragraph 80.3(2)(e) provides that a Court may take into account whether a person's acts were done with the intention of assisting persons specified in paragraphs 24AA(2)(a) of the Crimes Act. These paragraphs reflect the elements of the existing offence of treachery in section 24AA of the Crimes Act, which is being repealed by Item 43 of Schedule 1. These aspects of the treachery offence are not being replicated in the new offence of treachery proposed to be created in section 80.1AC through Item 4 of Schedule 1.

198. Following the repeal of the offence at section 24AA of the Crimes Act, it will not be necessary for a Court to be able to take these matters into account when considering a defence under subsection 80.3(1).

Item 7

199. Item 7 amends subsection 80.4(2) of the Criminal Code to insert the words 'section 80.1AC'. This has the effect of applying Section 15.4 (extended geographical jurisdiction—Category D) to the treachery offence in section 80.1AC of the Criminal Code (to be inserted by Item 4 of Schedule 1).

200. Under section 15.4, the effect of Category D geographical jurisdiction is that the offence applies:

- whether or not the conduct constituting the alleged offence occurs in Australia, and
- whether or not a result of the conduct constituting the alleged offence occurs in Australia.

201. Category D jurisdiction is appropriate because acts of force or violence intended to overthrow the Constitution, the Government of the Commonwealth or of a State or Territory or the lawful authority of the Government of the Commonwealth can pose a threat to Australia regardless of where the conduct constituting the offence occurs.

Item 8

202. Item 8 inserts new Division 82 – Sabotage at the end of Part 5.1 of the Criminal Code. The Commonwealth's current sabotage offence (section 24AB of the Crimes Act) was introduced in 1960 and has not evolved to reflect the modern threat environment. The existing sabotage offence only protects Defence facilities.

Division 82 - Sabotage

Section 82.1 – Definitions

203. Section 82.1 inserts definitions relevant to the sabotage offences in Division 82.

204. Conduct will result in ***damage to public infrastructure*** if any of the paragraphs in the definition apply in relation to ***public infrastructure*** (as defined in section 82.2). The paragraphs in the definition are:

- the conduct destroys it or results in its destruction
- the conduct involves interfering with it, or abandoning it, resulting in it being lost or rendered unserviceable
- the conduct results in it suffering a loss of function or becoming unsafe or unfit for its purpose
- the conduct limits or prevents access to it or any part of it by persons who are ordinarily entitled to access it or that part of it
- the conduct results in it or any part of it becoming defective or being contaminated
- the conduct significantly degrades its quality, or
- if it is an electronic system—the conduct seriously disrupts it.

205. Section 82.1 defines ***foreign principal*** as having the meaning given by section 90.2. Section 90.2 provides that each of the following is a ***foreign principal***:

- a foreign government principal
- a public international organisation
- a terrorist organisation within the meaning of Division 102 (see section 102.1)
- an entity or organisation directed or controlled by:
    - a public international organisation
    - a terrorist organisation within the meaning of Division 102
- an entity or organisation directed or controlled by two or more foreign principals within the meaning of any other paragraph of the definition.

206. The definition of ***foreign principal*** in section 90.2 is explained in detail at Item 16 of Schedule 1.

207. Section 82.1 defines ***national security*** as having the meaning given by section 90.4. Section 90.4 provides that the national security of Australia or a foreign country means:

- the defence of the country
- the protection of the country or any part of it, or the people of the country or any part of it, from activities covered by subsection 90.4(2)
- the protection of the integrity of the country's territory and borders from serious threats
- the carrying out of the country's responsibilities to any other country in relation to the protection of the integrity of the country's territory and borders from serious threats and the activities covered by subsection 90.4(2), and
- the country's political, military or economic relations with another country or other countries.

208. Subsection 90.4(2) provides that, for the purposes of subsection 90.4(1), this subsection covers the following activities relating to a country, whether or not directed from, or committed within, the country:

- espionage
- sabotage
- terrorism
- political violence
- activities intended and likely to obstruct, hinder or interfere with the performance by the country's defence force of its functions or with the carrying out of other activities by or for the country for the purposes of its defence or safety, and
- foreign interference.

209. Section 82.1 defines ***public infrastructure*** to have the meaning given by section 82.2. Section 82.2 defines ***public infrastructure*** to mean any of the following:

- any infrastructure, facility, premises, network or electronic system that belongs to the Commonwealth
- defence premises within the meaning of Part VIA of the Defence Act
- service property and service land, within the meaning of the Defence Force Discipline Act
- any part of the infrastructure of a telecommunications network within the meaning of the Telecommunications Act, and
- any infrastructure, facility, premises, network or electronic system (including an information, telecommunications or financial system) that:

- provides or relates to providing the public with utilities or services (including transport of people or goods) of any kind
- is located in Australia, and
- belongs to or is operated by a constitutional corporation or is used to facilitate constitutional trade and commerce.

210. The definition of public infrastructure covers infrastructure and services that are essential to everyday life in Australia. A disruption to public infrastructure due to sabotage could have a range of serious implications for business, governments and the community.

Section 82.2 – Public infrastructure

211. Section 82.2 sets out a definition of ***public infrastructure*** for the purpose of the sabotage offences in Division 82.

212. Paragraph 82.2(1)(a) deals with any infrastructure, facility, premises, network or electronic system that belongs to the Commonwealth.

- *Infrastructure* is not defined and is intended to take its ordinary meaning, which would include the structures and facilities needed for the operation of society.
- *Facilities* is not defined and is intended to take its ordinary meaning, which would include a place, amenity or piece of equipment.
- *Premises* is not defined and is intended to take its ordinary meaning, which would include a building, together with its land, occupied by a business or used in an official context.
- *Network* is not defined and is intended to take its ordinary meaning. This is primarily intended to cover networks of interconnected computers or other machines.
- *Electronic system* is not defined and is intended to take its ordinary meaning, which would include a physical interconnection of components or parts that gather various amounts of information together. This may include databases or software and may or may not be connected to other computers or machines as part of a *network*.

213. Consistent with subsection 82.2(1), the infrastructure, facility, premises, network or electronic system must ***belong*** to the Commonwealth. Subsection 82.2(2) provides that whether the property belongs to the Commonwealth is to be determined in the same way as it would be under Chapter 7 of the Criminal Code, specifically section 130.2 of the Criminal Code.

214. Under section 130.2, property ***belongs to*** a person if, and only if:

- the person has possession or control of the property

- the person has a proprietary right or interest in the property, other than an equitable interest arising only from:
    - an agreement to transfer an interest
    - an agreement to grant an interest, or
    - a constructive trust.

215. Paragraph 82.2(1)(b) deals with defence premises within the meaning of Part VIA of the Defence Act.

216. Section 71A of the Defence Act defines ***defence premises*** to mean any of the following that is in Australia, and is owned or occupied by the Commonwealth for use by the Defence Force or the Department:

- an area of land or any other place (whether or not it is enclosed or built on)
- a building or other structure
- a vehicle, vessel or aircraft, including any fixed or moveable ramp, stairs or other means of access to, or exit from, the vehicle, vessel or aircraft
- a prohibited area, within the meaning of the *Defence (Special Undertakings) Act 1952*, or
- Woomera Prohibited Area.

217. The Defence (Special Undertakings) Act defines a prohibited area as a place, or an area, that is a prohibited area under section 7, 8 or 8A.

- Section 7 defines a prohibited area as a place being used or occupied for the purpose of a special defence undertaking (as defined in section 6).
- Section 8 allows the Minister to declare a prohibited area if it is necessary for the purposes of the defence of the Commonwealth.
- Section 8A provides that the Joint Defence Facility Pine Gap is a prohibited area.

218. The Defence Act defines the Woomera Prohibited Area in section 72TA as an area prescribed by the Rules that is intended for use for the purposes of testing war materiel and may be used for those purposes. The *Woomera Prohibited Area Rule 2014* defines the Woomera Prohibited Area.

219. Paragraph 82.2(1)(c) deals with service property and service land within the meaning of the Defence Force Discipline Act.

220. Section 3 of the Defence Force Discipline Act defines ***service property*** as property used by, or in the possession or under the control of:

- the Defence Force

- an allied force (also defined in section 3 to mean a force of another country that is acting in cooperation with the Defence Force), or

- an institution of the Defence Force or of an allied force.

221. Section 3 of the Defence Force Discipline Act defines ***service land*** as land (including a building or other structure) used or occupied by:

- the Defence Force

- an allied force (also defined in section 3 to mean a force of another country that is acting in cooperation with the Defence Force), or

- an institution of the Defence Force or of an allied force.

222. Paragraph 82.2(1)(d) deals with any part of the infrastructure of a telecommunications network within the meaning of the Telecommunications Act.

223. Section 7 of the Telecommunications Act defines ***telecommunications network*** as a system, or series of systems, that carries, or is capable of carrying, communications by means of guided and/or unguided electromagnetic energy.

224. The reference in paragraph 82.2(1)(d) to 'any part of the infrastructure of a telecommunications network', is intended to clarify that the definition does not include customer cabling or equipment.

225. Paragraph 82.2(1)(e) deals with any infrastructure, facility, premises, network or electronic system (including an information, telecommunications or financial system) that:

- provides or relates to providing the public with utilities or services (including transport of people or goods) of any kind

- is located in Australia, and

- belongs to or is operated by a constitutional corporation or used to facilitate constitutional trade and commerce.

226. The terms 'infrastructure, facility, premises, network or electronic system' are described in detail in the explanation of paragraph 82.2(1)(a), above.

227. Paragraph 82.2(1)(e) is intended to cover essential services that are provided to the Australian community but do not belong to the Government. This would include private companies (that are a constitutional corporation within the existing definition of ***constitutional corporation*** in the Dictionary to the Criminal Code or are engaged in activities that facilitate constitutional trade and commerce within the definition to be inserted into the Dictionary to the Criminal Code by Item 24 of Schedule 1).

228. The Dictionary to the Criminal Code defines ***constitutional corporation*** as meaning a corporation to which paragraph 51(xx) of the Constitution applies.

229. Item 24 of Schedule 1 will insert a definition of ***constitutional trade and commerce*** into the Dictionary to the Criminal Code. The term will be defined to mean trade and commerce:

- with other countries
- among the States
- between a State and Territory, or
- between two Territories.

230. 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.

231. Subsection 82.2(2) provides that, for the purposes of the application of paragraphs 82.2(1)(a) (e) in relation to property within the meaning of Chapter 7, whether the property ***belongs*** to the Commonwealth or a constitutional corporation is to be determined in the same way as it would be under Chapter 7. The effect of section 130.2 is described above in relation to paragraph 82.2(1)(a).

232. Subsection 82.2(3) provides that, for the purposes of a reference in an element of an offence to public infrastructure (within the meaning of Division 82), absolute liability applies:

- in relation to public infrastructure within the meaning of paragraph (1)(a) of the definition – to the element that the infrastructure, facility, premises, network or electronic system belongs to the Commonwealth, and
- in relation to public infrastructure within the meaning of paragraph (1)(e) – to the element that the infrastructure, facility, premises, network or electronic system belongs to or is operated by a constitutional corporation or is used to facilitate constitutional trade and commerce.

233. It is appropriate to apply absolute liability to offences that rely on paragraphs 82.2(1)(a) or (e) because these are jurisdictional elements. A jurisdictional element of the offence is an element that does not relate to the substance of the offence, but marks a jurisdictional boundary between matters that fall within the legislative power of the Commonwealth and those that do.

234. The application of absolute liability to the element of the offence that the infrastructure 'belongs' to the Commonwealth is consistent with other offences dealing with property belonging to the Commonwealth. For example, section 131.1 of the Criminal Code (dealing with theft of Commonwealth property) applies absolute liability to the element of the offence that the property belongs to a Commonwealth entity.

235. Similarly, it is consistent with existing offences in the Criminal Code to apply absolute liability to offences dealing with activities undertaken by constitutional corporations or that facilitate constitutional trade and commerce. For example, section 380.2 of the

Criminal Code (dealing with contaminating goods) applies absolute liability to the element of the offence relevant to constitutional corporations and facilitating constitutional trade and commerce (subsection 380.2(3)).

236. The implications of applying absolute liability to the relevant elements of the sabotage offences are considered below in the discussion of each offence.

Section 82.3 – Offence of sabotage involving foreign principal with intention as to national security

237. Subsection 82.3(1) will make it an offence to engage in conduct on behalf of a foreign principal or directed, funded or supervised by a foreign principal, that results in damage to public infrastructure, with an intention to prejudice Australia's national security or advantage the national security of a foreign country.

238. This offence will be punishable by a maximum penalty of 25 years imprisonment.

239. An example of this offence is as follows. Person A is an employee of Country B, an adversary of Australia. At the direction of Country B, Person A gains access to a sensitive Defence facility and damages electronic equipment, meaning that the Australian Defence Force is unable to undertake essential satellite monitoring. Person A intended that the damage to the equipment would advantage the national security of Country B by enabling it to undertake missile launches without timely detection by the Australian Government.

240. To establish this offence, the prosecution will need to prove, beyond a reasonable doubt, that:

- a person intentionally engages in conduct
- the person's conduct results in damage to public infrastructure and the person is reckless as to this element
- the person intends that their conduct will prejudice Australia's national security or advantage the national security of a foreign country
- the conduct was engaged in:
    - on behalf of, or in collaboration with, a foreign principal or a person acting on behalf of a foreign principal and the person was reckless as to this, or
    - the conduct was directed, funded or supervised by a foreign principal or a person acting on behalf of a foreign principal and the person was reckless as to this.

241. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraphs 82.3(1)(a). Intention is also the fault element in relation to paragraph 82.3(1) c). Under subsection 5.2(1) of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

242. Recklessness is the fault element applying to paragraphs 82.3(1)(b) and (d). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and

- a result if he or she is 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 the risk.

243. For paragraph 82.3(1)(a) of the offence, the prosecution will have to prove beyond a reasonable doubt that the defendant intended to engage in the relevant conduct. Consistent with subsection 4.1(2) of the Criminal Code, the reference to 'engages in conduct' in paragraph 82.3(1)(a) means to do an act or to omit to perform an act.

244. For paragraph 82.3(1)(b) of the offence, the prosecution will have to prove, beyond a reasonable doubt, that the person's conduct resulted in damage to public infrastructure and that the person was reckless as to this element. Therefore, the defendant must have been aware of a substantial risk that their act or omission would result in damage to public infrastructure and that, having regard to the circumstances known to him or her that it is unjustifiable to take that risk.

245. Paragraph 82.3(1)(b) refers to conduct that results in ***damage to public infrastructure,*** which section 82.1 defines to mean any of the following in relation to public infrastructure:

- the conduct destroys it or results in its destruction

- the conduct involves interfering with it, or abandoning it, resulting in it being lost or rendered unserviceable

- the conduct results in it suffering a loss of function or becoming unsafe or unfit for its purpose

- the conduct limits or prevents access to it or any part of it by persons who are ordinarily entitled to access it or that part of it

- the conduct results in it or any part of it becoming defective or being contaminated

- the conduct significantly degrades its quality, or

- if it is an electronic system—the conduct seriously disrupts it.

246. Section 82.2 defines ***public infrastructure*** to mean any of the following:

- any infrastructure, facility, premises, network or electronic system that belongs to the Commonwealth

- defence premises within the meaning of Part VIA of the Defence Act

- service property and service land, within the meaning of the Defence Force Discipline Act

- any part of the infrastructure of a telecommunications network within the meaning of the *Telecommunications Act 1997*, and

- any infrastructure, facility, premises, network or electronic system (including an information, telecommunications or financial system) that:

    - provides or relates to providing the public with utilities or services (including transport of people or goods) of any kind

    - is located in Australia, and

    - belongs to or is operated by a constitutional corporation or used to facilitate constitutional trade and commerce.

247. To the extent that the prosecution is relying on paragraph 82.2(1)(a) of the definition of ***public infrastructure***, absolute liability will apply to the element that the infrastructure, facility or premises, network or electronic system belongs to the Commonwealth. To the extent that the prosecution is relying on paragraph 82.2(1)(e) of the definition of ***public infrastructure***, absolute liability will apply to the element that the infrastructure, facility or premises, network or electronic system belongs to, or is operated by, a constitutional corporation or is used to facilitate constitutional trade or commerce.

248. It is appropriate to apply absolute liability to these matters because these are jurisdictional elements. A jurisdictional element of the offence is an element that does not relate to the substance of the offence, but marks a jurisdictional boundary between matters that fall within the legislative power of the Commonwealth and those that do. This is consistent with Commonwealth criminal law practice, as described in the Guide to Framing Commonwealth Offences.

249. Absolute liability is set out in section 6.2 of the Criminal Code. The effect of applying absolute liability to an element of an offence is that no fault element needs to be proved and the defence of mistake of fact is unavailable. Accordingly, the prosecution will be required to prove only the physical element that the relevant infrastructure:

- belongs to the Commonwealth

- belongs to a constitutional corporation

- is operated by a constitutional corporation, or

- is used to facilitate constitutional trade or commerce.

250. For paragraph 82.3(1)(c) of the offence, the prosecution will have to prove beyond a reasonable doubt that the defendant intended for their act or omission to prejudice Australia's national security or advantage the national security of a foreign country. The ***national security*** of Australia or a foreign country is defined in section 90.4 and covers a broad range of possible prejudice to Australia's national security, such as damage to Australia's defence operations or harm to Australia's international relations.

251. The term 'prejudice' is intended to capture a broad range of intended conduct, including an intention to harm or injure Australia's national security or to cause disadvantage

to Australia. The term is also intended to cover impairment or loss to Australia's national security interests. 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.

252. The term 'advantage' is intended to capture an intention to put another country's national security in a favourable or superior position compared to Australia's position or to benefit or profit another's country's national security compared to Australia's national security.

253. Whether or not the prejudice to Australia's national security or advantage to the national security of a foreign country occurs or the conduct is capable of bringing it about is not relevant to the defendant's culpability for the offence. For example, the equipment that Person A damaged may not have been capable of disabling the satellite monitoring system, and therefore Person A's conduct was not capable of advantaging the national security of Country B.

254. For subparagraph 82.3(1)(c)(ii), the person must intend to advantage the national security of a 'foreign country', not a 'foreign principal'. This is because the interests of nation states in relation to 'national security' are unique and often relate to the protection to the territory of the country.

255. ***Foreign country*** is intended to cover countries other than Australia and is defined in the Dictionary to the Criminal Code as including:

- a colony or overseas territory
- a territory outside Australia, where a foreign country is to any extent responsible for the international relations of the territory, and
- a territory outside Australia that is, to some extent self-governing, but that is not recognised as an independent sovereign state by Australia.

256. Consistent with subsection 82.3(2), for the purposes of subparagraph 82.3(1)(c)(ii), the person does not need to have in mind a particular foreign country and may have in mind more than one foreign country. For example, a person's conduct may be directed by a foreign political organisation (which falls within the definition of ***foreign principal*** in section 90.) and may be aware of a substantial risk that their conduct will advantage the national security of a foreign country but will not know, or necessarily care, which foreign country that is. Similarly, a person may intend to advantage the national security of more than one foreign country by damaging Australian public infrastructure.

257. For paragraph 82.3(1)(d) the prosecution will have to prove beyond a reasonable doubt that the defendant's conduct was engaged in on behalf of, or in collaboration with, a foreign principal (as defined in section 90.), on behalf of, or in collaboration with, a person acting on behalf of a foreign principal, directed, funded or supervised by a foreign principal or a person acting on behalf of a foreign principal. The prosecution will also have to prove that the person was reckless as to this element. Therefore, the person must be aware of a substantial risk that their act or omission was engaged in on behalf of, or in collaboration with, a foreign principal, on behalf of, or in collaboration with, a person acting on behalf of a foreign principal, directed, funded or supervised by a foreign principal or a person acting on

behalf of a foreign principal, or and that, having regard to the circumstances known to him or her that it is unjustifiable to take that risk.

258. For subparagraph 82.3(1)(d)(i), the term 'on behalf of' is intended to include where a person or entity represents, acts in the interests of, or acts as a proxy for, a foreign government principal.

259. It is possible that a defendant will know, or be reckless, as to the fact that they are engaging in conduct for a foreign government because they are being tasked by a person who identifies himself or herself as an official of a foreign government. In this case, the person will be engaging in the conduct on behalf of the foreign principal.

260. However, it may also be the case that the defendant is not tasked directly by a foreign government official, but by an intermediary. In this case, the prosecution will have to prove beyond a reasonable doubt that the defendant was aware of a substantial risk that he or she was being tasked by a person acting on behalf of a foreign principal and that it was unjustifiable to take that risk. This may be the case where, for example, the intermediary advises the defendant that the intermediary acts in coordination with foreign officials, or the intermediary facilitates preferential treatment for the defendant from a foreign government.

261. Consistent with subsection 82.3(3), for the purposes of paragraph 82.3(1)(d), the person will not need to have in mind a particular foreign principal and may have in mind more than one foreign principal. For example, a defendant may assist an individual who has identified themselves to the defendant as a foreign official, but has not specified which foreign country they represent. Or, a defendant may provide assistance in the knowledge this assistance will or could assist multiple foreign principals at the same time.

262. The maximum penalty for the offence in section 82.3 is 25 years imprisonment. The commission of this offence would have serious consequences for the sovereignty and national security of Australia. It is unacceptable for foreign principals to seek to damage Australia's public infrastructure. In the worst case scenario, Australians could be killed or seriously harmed as a result of damage caused to public infrastructure by a person acting on behalf of a foreign principal intending to harm Australia's national security. This justifies the serious maximum penalty for the offence.

263. The Note to section 82.3 notes that an alternative verdict may be available for an offence against section 82.3. The alternative verdicts for sabotage offences are set out at section 82.12.

Section 82.4 – Offence of sabotage involving foreign principal reckless as to national security

264. Subsection 82.4(1) will make it an offence to engage in conduct on behalf of, or in collaboration with, a foreign principal or directed, funded or supervised by a foreign principal, that results in damage to public infrastructure, reckless as to whether the conduct will prejudice Australia's national security or advantage the national security of a foreign country.

265. The offence will be punishable by a maximum penalty of 20 years imprisonment.

266. An example of this offence is as follows. Person C is an employee of Country D, an adversary of Australia. At the direction of Country D, Person C damages electricity

substations in Canberra, interrupting the power supply to several parts of the city, including areas in which Commonwealth departments are located. Person C is aware that the damage to the equipment is likely to prevent the Department of Defence and Australian intelligence agencies from operating.

267. To establish the offence, the prosecution will need to prove, beyond a reasonable doubt, that:

- a person intentionally engages in conduct
- the person's conduct results in damage to public infrastructure and the person is reckless as to this element
- the person is reckless as to whether their conduct will prejudice Australia's national security or advantage the national security of a foreign country
- the conduct was engaged in:
    - on behalf of, or in collaboration with, a foreign principal or a person acting on behalf of a foreign principal and the person was reckless as to this, or
    - the conduct was directed, funded or supervised by a foreign principal or a person acting on behalf of a foreign principal and the person was reckless as to this.

268. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 82.4(1)(a). Under subsection 5.2(1) of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

269. Recklessness is the fault element for paragraphs 82.4(1)(b), (c) and (d). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and
- a result if he or she is 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 the risk.

270. For paragraph 82.4(1)(a) of the offence, the prosecution will have to prove beyond a reasonable doubt that the defendant intended to engage in the relevant conduct. Consistent with subsection 4.1(2) of the Criminal Code, the reference to 'engages in conduct' in paragraph 82.4(1)(a) means to do an act or to omit to perform an act.

271. For paragraph 82.4(1)(b) of the offence, the prosecution will have to prove, beyond a reasonable doubt, that the person's conduct resulted in damage to public infrastructure and that the person was reckless as to this element. Therefore, the defendant must have been aware of a substantial risk that their act or omission would result in damage to public

infrastructure and that, having regard to the circumstances known to him or her that it is unjustifiable to take that risk.

272. Paragraph 82.4(1)(b) refers to conduct that results in ***damage to public infrastructure,*** which section 82.1 defines to mean any of the following in relation to public infrastructure:

- the conduct destroys it or results in its destruction
- the conduct involves interfering with it, or abandoning it, resulting in it being lost or rendered unserviceable
- the conduct results in it suffering a loss of function or becoming unsafe or unfit for its purpose
- the conduct limits or prevents access to it or any part of it by persons who are ordinarily entitled to access it or that part of it
- the conduct results in it or any part of it becoming defective or being contaminated
- the conduct significantly degrades its quality, or
- if it is an electronic system—the conduct seriously disrupts it.

273. Section 82.2 defines ***public infrastructure*** to mean any of the following:

- any infrastructure, facility, premises, network or electronic system that belongs to the Commonwealth
- defence premises within the meaning of Part VIA of the Defence Act
- service property and service land, within the meaning of the Defence Force Discipline Act
- any part of the infrastructure of a telecommunications network within the meaning of the Telecommunications Act, and
- any infrastructure, facility, premises, network or electronic system (including an information, telecommunications or financial system) that:
    - provides or relates to providing the public with utilities or services (including transport of people or goods) of any kind
    - is located in Australia, and
    - belongs to or is operated by a constitutional corporation or used to facilitate constitutional trade and commerce.

274. To the extent that the prosecution is relying on paragraph 82.2(1)(a) of the definition of ***public infrastructure***, absolute liability will apply to the element that the infrastructure, facility or premises, network or electronic system belongs to the Commonwealth. To the extent that the prosecution is relying on paragraph 82.2(1)(e) of the definition of

public infrastructure, absolute liability will apply to the element that the infrastructure, facility or premises, network or electronic system belongs to, or is operated by, a constitutional corporation or is used to facilitate constitutional trade or commerce.

275. It is appropriate to apply absolute liability to these matters because these are jurisdictional elements. A jurisdictional element of the offence is an element that does not relate to the substance of the offence, but marks a jurisdictional boundary between matters that fall within the legislative power of the Commonwealth and those that do. This is consistent with Commonwealth criminal law practice, as described in the Guide to Framing Commonwealth Offences.

276. Absolute liability is set out in section 6.2 of the Criminal Code. The effect of applying absolute liability to an element of an offence is that no fault element needs to be proved and the defence of mistake of fact is unavailable. Accordingly, the prosecution will be required to prove only the fact that the relevant infrastructure:

- belongs to the Commonwealth
- belongs to a constitutional corporation
- is operated by a constitutional corporation, or
- is used to facilitate constitutional trade or commerce.

277. For paragraph 82.4(1)(c) of the offence, the prosecution will have to prove beyond a reasonable doubt that the defendant was aware of a substantial risk that their act or omission would prejudice to Australia's national security or advantage the national security of a foreign country and that, having regard to the circumstances known to him or her that it is unjustifiable to take that risk.

278. ***National security*** is defined in section 90.4 and covers a broad range of possible prejudice to Australia's national security, such as damage to Australia's defence operations or harm to Australia's international relations.

279. The term 'prejudice' is intended to capture a broad range of intended conduct, including an intention to harm or injure Australia's national security or to cause disadvantage to Australia. The term is also intended to cover impairment or loss to Australia's national security interests. 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.

280. The term 'advantage' is intended to capture an intention to put another country's national security in a favourable or superior position compared to Australia's position or to benefit or profit another's country's national security compared to Australia's national security.

281. Whether or not the prejudice to Australia's national security or advantage to a foreign country's national security occurs or the conduct is capable of bringing it about is not relevant to the defendant's culpability for the offence. For example, the departments and agencies that Person C intended to prevent from operating may have had power available

from generators and their power supply may not have been interrupted and therefore Person C's conduct was not capable of prejudicing Australia's national security.

282. For subparagraph 82.4(1)(c)(ii), the person must be reckless as to whether his or her conduct will advantage the national security of a 'foreign country', not a 'foreign principal'. This is because the interests of nation states in relation to 'national security' are unique and often relate to the protection to the territory of the country.

283. ***Foreign country*** is intended to cover countries other than Australia and is defined in the Dictionary to the Criminal Code as including:

- a colony or overseas territory
- a territory outside Australia, where a foreign country is to any extent responsible for the international relations of the territory, and
- a territory outside Australia that is, to some extent self-governing, but that is not recognised as an independent sovereign state by Australia.

284. Consistent with subsection 82.4(2), for the purposes of subparagraph 82.4(1)(c)(ii), the person does not need to have in mind a particular foreign country and may have in mind more than one foreign country. For example, a person's conduct may be directed by a foreign political organisation (which falls within the definition of ***foreign principal*** in section 90.) and may be aware of a substantial risk that their conduct will advantage the national security of a foreign country but will not know, or necessarily care, which foreign country that is. Similarly, a person may intend to advantage the national security of more than one foreign country by damaging Australian public infrastructure.

285. For paragraph 82.4(1)(d) the prosecution will have to prove beyond a reasonable doubt that the defendant's conduct was engaged in on behalf of, or in collaboration with, a foreign principal (as defined in section 90.), on behalf of, or in collaboration with, a person acting on behalf of a foreign principal, directed, funded or supervised by a foreign principal or a person acting on behalf of a foreign principal. The prosecution will also have to prove that the person was reckless as to this element. Therefore, the person must be aware of a substantial risk that their act or omission was engaged in on behalf of, or in collaboration with, a foreign principal, on behalf of, or in collaboration with, a person acting on behalf of a foreign principal, directed, funded or supervised by a foreign principal or a person acting on behalf of a foreign principal, or and that, having regard to the circumstances known to him or her that it is unjustifiable to take that risk.

286. It is possible that a defendant will know, or be reckless, as to the fact that they are engaging in conduct for a foreign principal because they are being tasked by a person who identifies himself or herself as an official of a foreign government. In this case, the person will be engaging in the conduct on behalf of the foreign principal.

287. However, it may also be the case that the defendant is not tasked directly by a foreign government official, but by an intermediary. In this case, the prosecution will have to prove beyond a reasonable doubt that the defendant was aware of a substantial risk that he or she was being tasked by a person acting on behalf of a foreign principal and that it was unjustifiable to take that risk. This may be the case where, for example, the intermediary

advises the defendant that the intermediary acts in coordination with foreign officials, or the intermediary facilitates preferential treatment for the defendant from a foreign government.

288. Consistent with subsection 82.4(3), for the purposes of paragraph 82.4(1)(d), the person will not need to have in mind a particular foreign principal and may have in mind more than one foreign principal. For example, a defendant may assist an individual who has identified themselves to the defendant as a foreign official, but has not specified which foreign country they represent. Or, a defendant may provide assistance in the knowledge this assistance will or could assist multiple foreign principals at the same time.

289. The maximum penalty for the offence in section 82.4 is 20 years imprisonment. It is unacceptable for foreign principals to seek to damage Australia's public infrastructure, reckless as to whether it will prejudice Australia's national security or advantage the national security of a foreign country. In the worst case scenario, Australians could be killed or seriously harmed as a result of damage to public infrastructure. This justifies the serious maximum penalty for the offence.

290. The Note to section 82.4 notes that an alternative verdict may be available for an offence against section 82.3. The alternative verdicts for sabotage offences are set out at section 82.12.

Section 82.5 – Offence of sabotage with intention as to national security

291. Section 82.5 will make it an offence to engage in conduct that results in damage to public infrastructure, with an intention to prejudice Australia's national security or advantage the national security of a foreign country.

292. The offence will be punishable by a maximum penalty of 20 years imprisonment.

293. An example of this offence is as follows. Person E is an employee of a Defence contractor. Person E is entitled to access highly sensitive Defence systems and uses that access to take the system offline at a critical point in a Defence operation. Person E is aware of the ongoing operation and knows that the system is essential to the success of the operation.

294. To establish the offence, the prosecution will need to prove, beyond a reasonable doubt, that:

- the person intentionally engages in conduct
- the conduct results in damage to public infrastructure and the person is reckless as to this element, and
- the person intends that his or her conduct will prejudice Australia's national security or advantage the national security of a foreign country.

295. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 82.5(1)(a). Intention is also the fault element for paragraph 82.5(1)(c). Under subsection 5.2(1) of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

296. Recklessness is the fault element for paragraph 82.5(1)(b). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and

- a result if he or she is 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 the risk.

297. For paragraph 82.5(1)(a) of the offence, the prosecution will have to prove beyond a reasonable doubt that the defendant intended to engage in the relevant conduct. Consistent with subsection 4.1(2) of the Criminal Code, the reference to 'engages in conduct' in paragraph 82.4(1)(a) means to do an act or to omit to perform an act.

298. For paragraph 82.5(1)(b) of the offence, the prosecution will have to prove, beyond a reasonable doubt, that the person's conduct resulted in damage to public infrastructure and that the person was reckless as to this element. Therefore, the defendant must have been aware of a substantial risk that their act or omission would result in damage to public infrastructure and that, having regard to the circumstances known to him or her that it is unjustifiable to take that risk.

299. Paragraph 82.5(1)(b) refers to conduct that results in ***damage to public infrastructure,*** which section 82.1 defines to mean any of the following in relation to public infrastructure:

- the conduct destroys it or results in its destruction

- the conduct involves interfering with it, or abandoning it, resulting in it being lost or rendered unserviceable

- the conduct results in it suffering a loss of function or becoming unsafe or unfit for its purpose

- the conduct limits or prevents access to it or any part of it by persons who are ordinarily entitled to access it or that part of it

- the conduct results in it or any part of it becoming defective or being contaminated

- the conduct significantly degrades its quality, or

- if it is an electronic system—the conduct seriously disrupts it.

300. Section 82.2 defines ***public infrastructure*** to mean any of the following:

- any infrastructure, facility, premises, network or electronic system that belongs to the Commonwealth

- defence premises within the meaning of Part VIA of the Defence Act

- service property and service land, within the meaning of the Defence Force Discipline Act

- any part of the infrastructure of a telecommunications network within the meaning of the Telecommunications Act, and

- any infrastructure, facility, premises, network or electronic system (including an information, telecommunications or financial system) that:

    - provides or relates to providing the public with utilities or services (including transport of people or goods) of any kind

    - is located in Australia, and

    - belongs to or is operated by a constitutional corporation or used to facilitate constitutional trade and commerce.

301. To the extent that the prosecution is relying on paragraph 82.2(1)(a) of the definition of ***public infrastructure***, absolute liability will apply to the element that the infrastructure, facility or premises, network or electronic system belongs to the Commonwealth. To the extent that the prosecution is relying on paragraph 82.2(1)(e) of the definition of ***public infrastructure***, absolute liability will apply to the element that the infrastructure, facility or premises, network or electronic system belongs to, or is operated by, a constitutional corporation or is used to facilitate constitutional trade or commerce.

302. It is appropriate to apply absolute liability to these matters because these are jurisdictional elements. A jurisdictional element of the offence is an element that does not relate to the substance of the offence, but marks a jurisdictional boundary between matters that fall within the legislative power of the Commonwealth and those that do. This is consistent with Commonwealth criminal law practice, as described in the Guide to Framing Commonwealth Offences.

303. Absolute liability is set out in section 6.2 of the Criminal Code. The effect of applying absolute liability to an element of an offence is that no fault element needs to be proved and the defence of mistake of fact is unavailable. Accordingly, the prosecution will be required to prove only the physical element that the relevant infrastructure:

- belongs to the Commonwealth

- belongs to a constitutional corporation

- is operated by a constitutional corporation, or

- is used to facilitate constitutional trade or commerce.

304. For paragraph 82.5(1)(c) of the offence, the prosecution will have to prove beyond a reasonable doubt that the defendant intended for their act or omission to prejudice Australia's ***national security*** or advantage the national security of a foreign country. The national security of Australia or a foreign country is defined in section 90.4 and covers a broad range of possible prejudice to Australia's national security, such as damage to Australia's defence operations or harm to Australia's international relations.

305. Whether or not the prejudice to Australia's national security or advantage to the national security of the foreign country occurs or the conduct is capable of bringing it about is not relevant to the defendant's culpability for the offence. For example, the system that Person E took offline may not actually have been essential to the mission and therefore Person E's conduct was not capable of prejudicing Australia's national security.

306. For subparagraph 82.5(1)(c)(ii), the person must intend to advantage the national security of a 'foreign country', not a 'foreign principal'. This is because the interests of countries in relation to 'national security' are unique and often relate to the protection to the territory of the country.

307. ***Foreign country*** is intended to cover countries other than Australia and is defined in the Dictionary to the Criminal Code as including:

- a colony or overseas territory
- a territory outside Australia, where a foreign country is to any extent responsible for the international relations of the territory, and
- a territory outside Australia that is, to some extent self-governing, but that is not recognised as an independent sovereign state by Australia.

308. Consistent with subsection 82.5(2), for the purposes of subparagraph 82.5(1)(c)(ii), the person does not need to have in mind a particular foreign country and may have in mind more than one foreign country. For example, a person's conduct may be directed by a foreign political organisation (which falls within the definition of ***foreign principal*** in section 90.) and may be aware of a substantial risk that their conduct will advantage the national security of a foreign country but will not know, or necessarily care, which foreign country that is. Similarly, a person may intend to advantage the national security of more than one foreign country by damaging Australian public infrastructure.

309. The maximum penalty for the offence in section 82.5 is 20 years imprisonment. The commission of this offence would have serious consequences for the sovereignty and national security of Australia. It is unacceptable for persons to seek to damage Australia's public infrastructure intending to prejudice Australia's national security or advantage the national security of a foreign principal. In the worst case scenario, Australians could be killed or seriously harmed as a result of infrastructure damage by a person intending to harm Australia's national security. This justifies the serious maximum penalty for the offence.

310. The Note to section 82.5 notes that an alternative verdict may be available for an offence against section 82.3. The alternative verdicts are set out at section 82.12.

Section 82.6 – Offence of sabotage reckless as to national security

311. Section 82.6 will make it an offence to engage in conduct that results in damage to public infrastructure, reckless as to whether that conduct will prejudice Australia's national security or advantage the national security of a foreign country.

312. The offence will be punishable by a maximum penalty of 15 years imprisonment.

313. An example of this offence is as follows. Person F places several locks on the gates of part of a Defence facility in a foreign country which is used as a base for troops involved in an international armed conflict. It would take up to 30 minutes to cut the locks off and gain access to the weapons. Person F is aware of an imminent planned attack on the Defence facility.

314. To establish the offence, the prosecution will need to prove, beyond a reasonable doubt, that:

- a person intentionally engages in conduct;
- the person's conduct results in damage to public infrastructure and the person is reckless as to this element, and
- the person is reckless as to whether the person's conduct will prejudice Australia's national security or advantage the national security of a foreign country.

315. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 82.6(1)(a). Under subsection 5.2(1) of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

316. Recklessness is the fault element of recklessness for paragraphs 82.6(1)(b) and (c). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and
- a result if he or she is 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 the risk.

317. For paragraph 82.6(1)(a) of the offence, the prosecution will have to prove beyond a reasonable doubt that the defendant intended to engage in the relevant conduct. Consistent with subsection 4.1(2) of the Criminal Code, the reference to 'engages in conduct' in paragraph 82.6(1)(a) means to do an act or to omit to perform an act.

318. For paragraph 82.6(1)(b) of the offence, the prosecution will have to prove, beyond a reasonable doubt, that the defendant was aware of a substantial risk that their act or omission would result in damage to public infrastructure and that, having regard to the circumstances known to him or her that it is unjustifiable to take that risk.

319. Paragraph 82.6(1)(b) refers to conduct that results in ***damage to public infrastructure,*** which subsection 82.1 defines to mean any of the following in relation to public infrastructure:

- the conduct destroys it or results in its destruction
- the conduct involves interfering with it, or abandoning it, resulting in it being lost or rendered unserviceable

- the conduct results in it suffering a loss of function or becoming unsafe or unfit for its purpose
- the conduct limits or prevents access to it or any part of it by persons who are ordinarily entitled to access it or that part of it
- the conduct results in it or any part of it becoming defective or being contaminated
- the conduct significantly degrades its quality, or
- if it is an electronic system—the conduct seriously disrupts it.

320. Section 82.2 defines ***public infrastructure*** to mean any of the following:

- any infrastructure, facility, premises, network or electronic system that belongs to the Commonwealth
- defence premises within the meaning of Part VIA of the Defence Act
- service property and service land, within the meaning of the Defence Force Discipline Act
- any part of the infrastructure of a telecommunications network within the meaning of the Telecommunications Act, and
- any infrastructure, facility, premises, network or electronic system (including an information, telecommunications or financial system) that:
    - provides or relates to providing the public with utilities or services (including transport of people or goods) of any kind
    - is located in Australia, and
    - belongs to or is operated by a constitutional corporation or used to facilitate constitutional trade and commerce.

321. To the extent that the prosecution is relying on paragraph 82.2(1)(a) of the definition of ***public infrastructure***, absolute liability will apply to the element that the infrastructure, facility or premises, network or electronic system belongs to the Commonwealth. To the extent that the prosecution is relying on paragraph 82.2(1)(e) of the definition of ***public infrastructure***, absolute liability will apply to the element that the infrastructure, facility or premises, network or electronic system belongs to, or is operated by, a constitutional corporation or is used to facilitate constitutional trade or commerce.

322. It is appropriate to apply absolute liability to these matters because these are jurisdictional elements. A jurisdictional element of the offence is an element that does not relate to the substance of the offence, but marks a jurisdictional boundary between matters that fall within the legislative power of the Commonwealth and those that do. This is consistent with Commonwealth criminal law practice, as described in the Guide to Framing Commonwealth Offences.

323. Absolute liability is set out in section 6.2 of the Criminal Code. The effect of applying absolute liability to an element of an offence is that no fault element needs to be proved and the defence of mistake of fact is unavailable. Accordingly, the prosecution will be required to prove only the fact that the relevant infrastructure:

- belongs to the Commonwealth
- belongs to a constitutional corporation
- is operated by a constitutional corporation, or
- is used to facilitate constitutional trade or commerce.

324. For paragraph 82.6(1)(c) of the offence, the prosecution will have to prove beyond a reasonable doubt that the defendant was aware of a substantial risk that their act or omission would prejudice Australia's ***national security*** or advantage the national security of a foreign country and that, having regard to the circumstances known to him or her that it is unjustifiable to take that risk. The national security of Australia or a foreign country is defined in section 90.4 and covers a broad range of possible prejudice to Australia's national security, such as damage to Australia's defence operations or harm to Australia's international relations.

325. The term 'prejudice' is intended to capture a broad range of intended conduct, including an intention to harm or injure Australia's national security or to cause disadvantage to Australia. The term is also intended to cover impairment or loss to Australia's national security interests. 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.

326. The term 'advantage' is intended to capture an intention to put another country's national security in a favourable or superior position compared to Australia's position or to benefit or profit another's country's national security compared to Australia's national security.

327. Whether or not prejudice to Australia's national security or advantage to the national security of a foreign country occurs or the conduct is capable of bringing it about is not relevant to the defendant's culpability for the offence. For example, the weapons which Person F has prevented Defence personnel from accessing may not be critical to protecting the facility from an attack and therefore Person F's conduct may not have been capable of prejudicing Australia's national security.

328. For subparagraph 82.6(1)(c)(ii), the person must be reckless as to whether his or her conduct will advantage the national security of a 'foreign country', not a 'foreign principal'. This is because the interests of nation states in relation to 'national security' are unique and often relate to the protection to the territory of the country.

329. ***Foreign country*** is intended to cover countries other than Australia and is defined in the Dictionary to the Criminal Code as including:

- a colony or overseas territory

- a territory outside Australia, where a foreign country is to any extent responsible for the international relations of the territory, and

- a territory outside Australia that is, to some extent self-governing, but that is not recognised as an independent sovereign state by Australia.

330. Consistent with subsection 82.6(2), for the purposes of subparagraph 82.6(1)(c), the person does not need to have in mind a particular foreign country and may have in mind more than one foreign country. For example, a person's conduct may be directed by a foreign political organisation (which falls within the definition of ***foreign principal*** in section 90.2 and may be aware of a substantial risk that their conduct will advantage the national security of a foreign country but will not know, or necessarily care, which foreign country that is. Similarly, a person may intend to advantage the national security of more than one foreign country by damaging Australian public infrastructure.

331. The maximum penalty for the offence in section 82.6 is 15 years imprisonment. The commission of this offence would have serious consequences for the sovereignty and national security of Australia. It is unacceptable for persons to seek to damage Australia's public infrastructure reckless as to whether his or her conduct would prejudice Australia's national security or advantage the national security of a foreign country. In the worst case scenario, Australians could be killed or seriously harmed as a result of infrastructure damage by a person reckless so to whether their conduct will harm Australia's national security. This justifies the serious maximum penalty for the offence.

Section 82.7 – Offence of introducing vulnerability with intention as to national security

332. Section 82.7 will make it an offence for a person to engage in conduct that results in an article, thing or software that is, or is part of, public infrastructure becoming vulnerable to misuse, impairment or unauthorised access or modification where the conduct is intended to prejudice Australia's national security, harm or prejudice Australia's economic interests, disrupt the functions of an Australian government or to damage public infrastructure.

333. The offence will be punishable by a maximum penalty of 15 years imprisonment.

334. An example of this offence is as follows. Person G is a subcontractor engaged to build a software system to be used by a Commonwealth department involved in national security. When building the system, Person G deliberately creates a backdoor through which an intrusion into the software will be possible in future. Person G intends that this will enable a person to hack into the system in future and extract data. Person G intends to sell information about this vulnerability to a foreign country in order to harm Australia's interests by enabling that country to use the vulnerability to access highly sensitive data.

335. To establish the offence, the prosecution will need to prove, beyond a reasonable doubt, that:

- a person intentionally engages in conduct

- the person's conduct has the result that an article or thing, or software becoming vulnerable to:

    - misuse or impairment, or

- to being accessed or modified by person not entitled to access or modify it

and the person is reckless as to this element

- the article or thing or software, is or is part of public infrastructure and the person is reckless as to this element

- the person engages in the conduct intending that, whether at the time or at a future time, that one of the following will occur:

  - prejudice to Australia's national security

  - harm or prejudice to Australia's economic interests

  - disruption to the functions of the Government of the Commonwealth, of a State or of a Territory, or

  - damage to public infrastructure.

336. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 82.7(a). Intention is also the fault element for paragraph 82.7(d). Under subsection 5.2(1) of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

337. Recklessness is the fault element for paragraphs 82.7(b) and (c). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and

- a result if he or she is 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 the risk.

338. For paragraph 82.7(a) of the offence, the prosecution will have to prove beyond a reasonable doubt that the defendant intended to engage in the relevant conduct. Consistent with subsection 4.1(2) of the Criminal Code, the reference to 'engages in conduct' in paragraph 82.7(a) means to do an act or to omit to perform an act.

339. For paragraph 82.7(b) of the offence, the prosecution will have to prove, beyond a reasonable doubt, that the defendant's conduct had the result that an article or thing or software becomes vulnerable to misuse or impairment or to being accessed or modified by a person not entitled to access or modify it. The person must be reckless as to this element. Therefore, the defendant must be aware of a substantial risk that their act or omission would result in an article, thing or software becoming vulnerable to misuse, impairment or access or modification by a person not entitled to access or modify it and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk.

340. For the purposes of paragraph 82.7(b):

- *Article* is intended to include substances and materials.
- *Thing* is intended to cover all objects.
- *Software* is intended to cover programs and operating systems used by computers.
- *Vulnerable* is intended to cover leaving the article, thing or software exposed to the possibility of being attacked or harmed.
- *Misuse* is intended to cover using something in the wrong way or for an unauthorised purpose.
- *Impairment* is intended to include weakening or damaging something or rendering it unusable.

341. For paragraph 82.7(c) of the offence, the prosecution will have to prove, beyond a reasonable doubt, that the article or thing or software is, or is part of, public infrastructure. The defendant must be reckless in relation to this element. Therefore, the defendant must have been aware of a substantial risk that the article, thing or software was part of public infrastructure and that, having regard to those circumstances, it is unjustifiable to take the risk.

342. Section 82.2 defines ***public infrastructure*** to mean any of the following:

- any infrastructure, facility, premises, network or electronic system that belongs to the Commonwealth
- defence premises within the meaning of Part VIA of the Defence Act
- service property and service land, within the meaning of the Defence Force Discipline Act
- any part of the infrastructure of a telecommunications network within the meaning of the Telecommunications Act, and
- any infrastructure, facility, premises, network or electronic system (including an information, telecommunications or financial system) that:
    - provides or relates to providing the public with utilities or services (including transport of people or goods) of any kind
    - is located in Australia, and
    - belongs to or is operated by a constitutional corporation or used to facilitate constitutional trade and commerce.

343. To the extent that the prosecution is relying on paragraph 82.2(1)(a) of the definition of ***public infrastructure***, absolute liability will apply to the element that the infrastructure, facility or premises, network or electronic system belongs to the Commonwealth. To the

extent that the prosecution is relying on paragraph 82.2(1)(e) of the definition of ***public infrastructure***, absolute liability will apply to the element that the infrastructure, facility or premises, network or electronic system belongs to, or is operated by, a constitutional corporation or is used to facilitate constitutional trade or commerce.

344. It is appropriate to apply absolute liability to these matters because these are jurisdictional elements. A jurisdictional element of the offence is an element that does not relate to the substance of the offence, but marks a jurisdictional boundary between matters that fall within the legislative power of the Commonwealth and those that do. This is consistent with Commonwealth criminal law practice, as described in the Guide to Framing Commonwealth Offences.

345. Absolute liability is set out in section 6.2 of the Criminal Code. The effect of applying absolute liability to an element of an offence is that no fault element needs to be proved and the defence of mistake of fact is unavailable. Accordingly, the prosecution will be required to prove only the physical element that the relevant infrastructure:

- belongs to the Commonwealth
- belongs to a constitutional corporation
- is operated by a constitutional corporation, or
- is used to facilitate constitutional trade or commerce.

346. For paragraph 82.7(d) of the offence, the prosecution will have to prove, beyond a reasonable doubt, that the defendant undertook their act or omission with the intention that any of the following would occur, whether at the time or at a future time:

- prejudice to Australia's national security,
- damage to Australia's economic interests,
- disruption to the functions of the Government of the Commonwealth, of a State or of a Territory or
- damage to public infrastructure.

347. Whether or not the one of these matters occurs or the conduct is capable of bringing it about is not relevant to the defendant's culpability for the offence. For example, Person G's backdoor in the relevant software may actually not allow for data to be extracted in the future.

348. Subparagraph 82.7(d)(i) refers to prejudice to Australia's national security. The term 'prejudice' is intended to capture a broad range of intended conduct, including an intention to harm or injure Australia's national security or to cause disadvantage to Australia. The term is also intended to cover impairment or loss to Australia's national security interests. 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.

349. The ***national security*** of Australia is defined in section 90.4 and covers a broad range of possible prejudice to Australia's national security, such as damage to Australia's defence operations or harm to Australia's international relations.

350. Subparagraph 82.7(d)(ii) refers to harm or prejudice to Australia's economic interests. The term 'prejudice' is intended to capture a broad range of intended conduct, including an intention to harm or injure Australia's economic interests or to cause disadvantage to Australia. The term is also intended to cover impairment or loss to Australia's economic interests. The prejudice to Australia's economic interests 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 on Australia's overall economy.

351. Paragraph 82.7(d)(iii) refers to disruption to the functions of the Government of the Commonwealth or of a State or Territory. This is intended to cover a disturbance or interruption to the functions of these governments. Although the disruption need not be serious or substantial, it is intended to be more than a minor or trivial disruption. The disruption may be to any of the functions of the Commonwealth or a State or Territory government.

352. Paragraph 82.7(d)(iv) refers to ***damage to public infrastructure,*** which section 82.1 defines to mean any of the following in relation to public infrastructure:

- the conduct destroys it or results in its destruction
- the conduct involves interfering with it, or abandoning it, resulting in it being lost or rendered unserviceable
- the conduct results in it suffering a loss of function or becoming unsafe or unfit for its purpose
- the conduct limits or prevents access to it or any part of it by persons who are ordinarily entitled to access it or that part of it
- the conduct results in it or any part of it becoming defective or being contaminated
- the conduct significantly degrades its quality, or
- if it is an electronic system—the conduct seriously disrupts it.

353. 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.

Section 82.8 – Offence of introducing vulnerability reckless as to national security

354. Section 82.8 will make it an offence for a person to engage in conduct that results in an article, thing or software that is or is part of public infrastructure becoming vulnerable to misuse, impairment or unauthorised access or modification where the person is reckless as to whether it will prejudice Australia's national security, harm or prejudice Australia's economic interests, disrupt the functions of an Australian government or damage public infrastructure.

355. The offence will be punishable by a maximum penalty of 10 years imprisonment.

356. An example of this offence is as follows. Person A works for the Australian Bureau of Statistics on the IT support helpdesk. Person A makes a change to security settings on the ABS's website that makes it vulnerable to a denial of service attack, and posts details of this vulnerability on a hacking noticeboard. Third parties conduct a denial of service using this vulnerability on the day that the ABS is scheduled to release important economic statistics, causing a loss of confidence and a severe drop in stock values across the Australian Stock Exchange. At the time they change the security settings, Person A is aware of the importance of the statistics to Australia's economy.

357. To establish the offence, the prosecution will need to prove, beyond a reasonable doubt, that:

- a person intentionally engages in conduct
- the person's conduct has the result that an article or thing, or software becoming vulnerable to:
    - misuse or impairment, or
    - to being accessed or modified by person not entitled to access or modify it

  and the person is reckless as to this element
- the article or thing or software, is or is part of public infrastructure and the person is reckless as to this element
- the person engages in the conduct reckless as to whether any of the following will occur (whether at the time or at a future time):
    - prejudice to Australia's national security
    - harm or prejudice to Australia's economic interests
    - disruption to the functions of the Government of the Commonwealth, of a State or of a Territory, or
    - damage to public infrastructure.

358. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 82.8(a). Under subsection 5.2(1) of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

359. Recklessness will be the fault element in relation to paragraphs 82.8(b), (c) and (d). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and

- a result if he or she is 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 the risk.

360. For paragraph 82.8(a) of the offence, the prosecution will have to prove beyond a reasonable doubt that the defendant intended to engage in the relevant conduct. Consistent with subsection 4.1(2) of the Criminal Code, the reference to 'engages in conduct' in paragraph 82.8(a) means to do an act or to omit to perform an act.

361. For paragraph 82.8(b) of the offence, the prosecution will have to prove, beyond a reasonable doubt, that the defendant's conduct had the result that an article, thing or software becomes vulnerable to misuse or impairment or to being accessed or modified by a person not entitled to access or modify it. Recklessness is the fault element for this element. Therefore, the defendant must have been aware of a substantial risk that their act or omission would result in an article, thing or software becoming vulnerable to misuse, impairment or access or modification by a person not entitled to access or modify it and, having regard to the circumstances known to him or her that it is unjustifiable to take that risk.

362. For the purposes of paragraph 82.8(b):

- *Article* is intended to include substances and materials.

- *Thing* is intended to cover all objects.

- *Software* is intended to cover programs and operating systems used by computers.

- *Vulnerable* is intended to cover leaving the article, thing or software exposed to the possibility of being attacked or harmed.

- *Misuse* is intended to cover using something in the wrong way or for an unauthorised purpose.

- *Impairment* is intended to include weakening or damaging something or rendering it unusable.

363. For paragraph 82.8(c) of the offence, the prosecution will have to prove, beyond a reasonable doubt, that the article or thing or software is or is part of public infrastructure and that, having regard to those circumstances, it is unjustifiable to take the risk. Recklessness is the fault element for this element. Therefore, the defendant must have been aware of a

substantial risk that the article, thing or software was part of public infrastructure and that, having regard to those circumstances, it is unjustifiable to take the risk.

364. Section 82.2 defines ***public infrastructure*** to mean any of the following:

- any infrastructure, facility, premises, network or electronic system that belongs to the Commonwealth
- defence premises within the meaning of Part VIA of the Defence Act
- service property and service land, within the meaning of the Defence Force Discipline Act
- any part of the infrastructure of a telecommunications network within the meaning of the Telecommunications Act, and
- any infrastructure, facility, premises, network or electronic system (including an information, telecommunications or financial system) that:
    - provides or relates to providing the public with utilities or services (including transport of people or goods) of any kind
    - is located in Australia, and
    - belongs to or is operated by a constitutional corporation or used to facilitate constitutional trade and commerce.

365. To the extent that the prosecution is relying on paragraph 82.2(1)(a) of the definition of ***public infrastructure***, absolute liability will apply to the element that the infrastructure, facility or premises, network or electronic system belongs to the Commonwealth. To the extent that the prosecution is relying on paragraph 82.2(1)(e) of the definition of ***public infrastructure***, absolute liability will apply to the element that the infrastructure, facility or premises, network or electronic system belongs to, or is operated by, a constitutional corporation or is used to facilitate constitutional trade or commerce.

366. It is appropriate to apply absolute liability to these matters because these are jurisdictional elements. A jurisdictional element of the offence is an element that does not relate to the substance of the offence, but marks a jurisdictional boundary between matters that fall within the legislative power of the Commonwealth and those that do. This is consistent with Commonwealth criminal law practice, as described in the Guide to Framing Commonwealth Offences.

367. Absolute liability is set out in section 6.2 of the Criminal Code. The effect of applying absolute liability to an element of an offence is that no fault element needs to be proved and the defence of mistake of fact is unavailable. Accordingly, the prosecution will be required to prove only the fact that the relevant infrastructure:

- belongs to the Commonwealth
- belongs to a constitutional corporation
- is operated by a constitutional corporation, or

- is used to facilitate constitutional trade or commerce.

368. For paragraph 82.8(d) of the offence, the prosecution will have to prove, beyond a reasonable doubt, that the defendant undertook their act or omission with the intention that any of the following would occur, whether at the time or at a future time:

- prejudice to Australia's national security,
- damage to Australia's economic interests,
- disruption to the functions of the Government of the Commonwealth, of a State or of a Territory or
- damage to public infrastructure.

369. Whether or not the one of these matters occurs or the conduct is capable of bringing it about is not relevant to the defendant's culpability for the offence. For example, Person G's backdoor in the relevant software may actually not allow for data to be extracted in the future.

370. Subparagraph 82.8(d)(i) refers to prejudice to Australia's national security. The term 'prejudice' is intended to capture a broad range of intended conduct, including an intention to harm or injure Australia's national security or to cause disadvantage to Australia. The term is also intended to cover impairment or loss to Australia's national security interests. 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.

371. The ***national security*** of Australia is defined in section 90.4 and covers a broad range of possible prejudice to Australia's national security, such as damage to Australia's defence operations or harm to Australia's international relations.

372. Subparagraph 82.8(d)(ii) refers to harm or prejudice to Australia's economic interests. The term 'prejudice' is intended to capture a broad range of intended conduct, including an intention to harm or injure Australia's economic interests or to cause disadvantage to Australia. The term is also intended to cover impairment or loss to Australia's economic interests. The prejudice to Australia's economic interests 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 on Australia's overall economy.

373. Paragraph 82.8(d)(iii) refers to disruption to the functions of the Government of the Commonwealth or of a State or Territory. This is intended to cover a disturbance or interruption to the functions of these governments. Although the disruption need not be serious or substantial, it is intended to be more than a minor or trivial disruption. The disruption may be to any of the functions of the Commonwealth or a State or Territory government.

374. Paragraph 82.8(d)(iv) refers to ***damage to public infrastructure,*** which section 82.1 defines to mean any of the following in relation to public infrastructure:

- the conduct destroys it or results in its destruction

- the conduct involves interfering with it, or abandoning it, resulting in it being lost or rendered unserviceable
- the conduct results in it suffering a loss of function or becoming unsafe or unfit for its purpose
- the conduct limits or prevents access to it or any part of it by persons who are ordinarily entitled to access it or that part of it
- the conduct results in it or any part of it becoming defective or being contaminated
- the conduct significantly degrades its quality, or
- if it is an electronic system—the conduct seriously disrupts it.

375. 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.

Section 82.9 – Offence of preparing for, or planning, a sabotage offence

376. Section 82.9 will establish a new offence of preparing for a sabotage offence. The new offence will criminalise conduct in preparation for, or planning, an offence against Division 82 (sabotage).

377. The offence will be punishable by a maximum penalty of seven years imprisonment.

378. An example of this offence is as follows. Person H intends to damage public infrastructure in another city. Person H has arranged travel to the city, has purchased the equipment needed to cause damage and has communicated with other people about his/her intention to damage the facility, including their intention to cause the damage in order to advantage a foreign country's national security.

379. The purpose of the offence is to give law enforcement authorities the means to deal with preparatory conduct and enable a person to be arrested before Australia's national security is prejudiced or the national security of a foreign country is advantaged.

380. To establish the offence, the prosecution will need to prove, beyond a reasonable doubt, that:

- a person intentionally engages in conduct, and
- the person does so with the intention of preparing for, or planning, an offence against Division 82 (sabotage).

381. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 82.9(1)(a). Under section 5.2 of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

382. For paragraph 82.9(1)(a), the prosecution will have to prove beyond a reasonable doubt that the defendant intentionally engaged in the relevant conduct. Consistent with subsection 4.1(2) of the Criminal Code, the reference to 'engages in conduct' in paragraph 82.9(1)(a) means to do an act or to omit to perform an act.

383. For paragraph 82.9(1)(b), the prosecution will have to prove beyond a reasonable doubt that the person engages in conduct with the intention of preparing for, or planning, an offence against Division 82 (sabotage). The terms preparing and planning are not defined and are intended to take their ordinary meanings.

- The term 'preparing' could include acts to conceive, formulate, make ready, arrange, and assemble an idea, plan, thing, or person for an offence against Division 82 (sabotage).

- The term 'planning' could include acts to organise, arrange, design, draft, or setup an idea, plan, thing, or person for an offence against Division 82 (sabotage).

384. Given the offences are directed at behaviour at the planning or preparation stage, it is appropriate to impose the fault element of intention on both of the elements of the offence. This will ensure that a person will only be guilty of this offence where there is sufficient evidence that the person intended to prepare for, or plan, a sabotage offence.

385. The maximum penalty for this offence is seven years imprisonment. While persons who attempt to commit offences are generally subject to the same penalty as if the actual offence had been carried out, the offence at subsection 82.9(1) is intended to capture behaviour at the planning stage, rather than the more advanced stage at which an ancillary offence of attempt could otherwise apply.

386. Subsection 82.9(2) specifies that section 11.1 (attempt) does not apply to an offence against subsection 82.9(1). Section 11.1 of the Criminal Code extends criminal responsibility for all Commonwealth offences and operates to automatically provide for ancillary offences such as attempting to commit an offence or inciting the commission of an offence. Subsection 82.9(2) modifies the automatic application of section 11.1 in relation to the ancillary offence of attempt. This is appropriate because the offence is already directed at conduct that is preparatory in nature.

387. Under paragraph 82.9(3)(a), the preparatory offence at subsection 82.9(1) will apply whether or not an offence against Division 82 is actually committed. This is consistent with the intention behind the offence to allow intervention by law enforcement prior to an act of sabotage occurring.

388. Under paragraph 82.9(3)(b), the preparatory offence at subsection 82.9(1) will apply whether or not the person engages in conduct in preparation for, or planning, a specific offence against a provision of Division 82. This clarifies that it is not necessary for the prosecution to identify a specific offence. It will be sufficient for the prosecution to prove that the particular conduct was related to 'an' offence. This ensures that the offence will be

available where a person has planned a range of activities preparatory to committing a sabotage offence that are still in the formative stages. For example, where a person has not necessarily decided on a particular target, time or date or other specific details that would constitute one of the specified offences against Division 82.

389. Under paragraph 82.9(3)(c), the preparatory offence at subsection 82.9(1) will apply whether or not the act is done in preparation for, or planning, more than one offence against a provision of Division 82. This clarifies that the offence will still apply where a person has engaged in preparatory conduct in relation to several sabotage offences.

Section 82.10 – Defence

390. The general defences available under Part 2.3 of the Criminal Code will be available to a person accused of an offence under Division 82. In addition, section 82.10 creates a specific defence.

391. Section 82.10 provides for a defence to prosecution for an offence against Division 82 if:

- the conduct the person engaged in was accessing or using a computer or other electronic system and
- the person engaged in the conduct in the person's capacity as a public official.

392. ***Public official*** is defined in the Dictionary to the Criminal Code to include:

- a Commonwealth public official
- an officer or employee of the Commonwealth or of a State or Territory
- an individual who performs work for the Commonwealth, or for a State or Territory, under a contract
- an individual who holds or performs the duties of an office established by a law of the Commonwealth or of a State or Territory
- an individual who is otherwise in the service of the Commonwealth or of a State or Territory (including service as a member of a military force or police force)
- a member of the executive, judiciary or magistracy of the Commonwealth or of a State or Territory, and
- an officer or employee of:
    - an authority of the Commonwealth, or
    - an authority of a State or Territory.

393. ***Commonwealth public official*** is defined in the Dictionary to the Criminal Code to mean:

- the Governor-General
- a person appointed to administer the Government of the Commonwealth under section 4 of the Constitution
- a Parliamentary Secretary
- a member of either House of the Parliament
- an individual who holds an appointment under section 67 of the Constitution
- the Administrator, an Acting Administrator, or a Deputy Administrator, of the Northern Territory
- a Commonwealth judicial officer (as defined in the Dictionary to the Criminal Code)
- an APS employee
- an individual employed by the Commonwealth other than under the *Public Service Act 1999*
- a member of the Australian Defence Force
- a member or special member of the AFP
- an individual (other than an official of a registered industrial organisation) who holds or performs the duties of an office established by or under a law of the Commonwealth, other than:
    - the *Corporations (Aboriginal and Torres Strait Islander) Act 2006*
    - the *Australian Capital Territory (Self-Government) Act 1988*
    - the *Corporations Act 2001*
    - the *Norfolk Island Act 1979*, or
    - the *Northern Territory (Self-Government) Act 1978*
- an officer or employee of a Commonwealth authority
- an individual who is a contracted service provider for a Commonwealth contract
- an individual who is an officer or employee of a contracted service provider for a Commonwealth contract and who provides services for the purposes (whether direct or indirect) of the Commonwealth contract

- an individual (other than an official of a registered industrial organisation) who exercises powers, or performs functions, conferred on the person by or under a law of the Commonwealth, other than:
    - the *Corporations (Aboriginal and Torres Strait Islander) Act 2006*
    - the *Australian Capital Territory (Self-Government) Act 1988*
    - the *Corporations Act 2001*
    - the *Norfolk Island Act 1979*
    - the *Northern Territory (Self-Government) Act 1978*, or
    - a provision specified in the regulations
- an individual who exercises powers, or performs functions, conferred on the person under a law in force in the Territory of Christmas Island or the Territory of Cocos (Keeling) Islands (whether the law is a law of the Commonwealth or a law of the Territory concerned), or
- the Registrar, or a Deputy Registrar, of Aboriginal and Torres Strait Islander Corporations.

394. An example of where this defence would apply would be where a Commonwealth department engages a contractor to conduct a penetration test of the department's electronic systems for vulnerabilities.

395. Note 1 under the defence at section 82.10 clarifies that the defendant will bear an evidentiary burden in relation to this offence. This is appropriate because the defendant should be readily able to point to evidence that the conduct engaged in was accessing or using a computer or other electronic system and was in their capacity as a public official.

396. Consistent with section 13.3 of the Criminal Code, the defendant bears the burden of adducing or pointing to evidence that suggests a reasonable possibility that the matter exists or does not exist. If the defendant discharges an evidential burden, the prosecution must disprove those matters beyond reasonable doubt, consistent with section 13.1 of the Criminal Code.

397. Both AFP and CDPP consider the availability of any defences when considering whether to investigate and prosecute criminal offences. In relation to prosecution decisions, the Prosecution Policy of the Commonwealth specifically requires the CDPP to take into account any lines of defence which are plainly open to, or have been indicated by, the alleged offender in deciding whether there is a reasonable prospect of a conviction being secured. Subsection 82.13(4) requires the Attorney-General consider whether the defendant's conduct is authorised under the defences in section 82.10 before providing his or her consent to the institution of proceedings for the commitment of a person for trial for an offence to which the defence applies.

Section 82.11 – Geographical jurisdiction

398. Section 82.11 applies Section 15.4 (extended geographical jurisdiction—Category D) to each offence against Division 82 (Sabotage). Under section 15.4, the effect of Category D geographical jurisdiction is that the offence applies:

- whether or not the conduct constituting the alleged offence occurs in Australia, and
- whether or not a result of the conduct constituting the alleged offence occurs in Australia.

399. Category D jurisdiction is appropriate because acts of sabotage may be undertaken from outside of Australia, particularly in relation to accessing software or electronic systems.

400. The application of Category D jurisdiction is consistent with other offences dealing with Commonwealth property, such as Part 7.2 of the Criminal Code.

401. Category D is also necessary to protect Defence facilities located outside Australia from sabotage.

Section 82.12 – Alternative verdicts

402. Subsection 82.12(1) provides that if the trier of fact is not satisfied that a person is guilty of an offence specific in column 1 (see table below) and is satisfied, beyond reasonable doubt, that the person is guilty of an offence against the corresponding offence specified in column 2 then it may find the person not guilty of the column 1 offence but guilty of the column 2 offence.

403. Subsection 82.12(2) provides that subsection 82.12(1) only applies if the person has been accorded procedural fairness in relation to the finding of guilt for the relevant offence specified in column 2.

Alternative verdicts

Item	Column 1 For an offence against:	Column 2 The alternative verdict is an offence against:
1	section 82.3 (sabotage involving foreign principal with intention as to national security)	any of the following: (a) section 82.4 (sabotage involving foreign principal reckless as to national security); (b) section 82.5 (sabotage with intention as to national security); (c) section 82.6 (sabotage reckless as to national security)
2	section 82.4 (sabotage involving foreign principal reckless as to national security)	section 82.6 (sabotage reckless as to national security)
3	section 82.5 (sabotage with intention as to national	section 82.6 (sabotage reckless as to national security)

Alternative verdicts		
Item	**Column 1** **For an offence against:**	**Column 2** **The alternative verdict is an offence against:**
	security)	
4	section 82.7 (introducing vulnerability with intention as to national security)	section 82.8 (introducing vulnerability reckless as to national security)

404. For example, if the defendant is on trial for an offence against new subsection 82.3 (offence of sabotage involving foreign principal with intention as to national security) and the jury is not satisfied that the defendant is guilty of an offence against that section, but is satisfied that he or she is guilty of an offence against new subsection 82.4 (offence of sabotage involving foreign principal reckless as to national security), it will be able to find the defendant guilty of the offence against section 82.4 instead.

Section 82.13 – Consent of Attorney-General required for prosecutions

405. Section 82.13 requires the written consent of the Attorney-General to commence proceedings against a person for offences in Division 82 of the Criminal Code, and is intended to ensure that there is appropriate oversight of prosecutions. This is appropriate given the seriousness of offences in Division 82 and the potential for national security or international considerations to arise.

406. 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 (CDPP) is not able to take into account under the *Prosecution Policy of the Commonwealth*.

407. Section 82.13 provides the Attorney-General opportunity to receive advice from relevant agencies and other Ministers about sensitivities that might arise if proceedings are commenced for offences under Division 82, and provides opportunity for consideration of whether the prosecution could be detrimental to Australia's foreign relations and national security. Section 82.13 is particularly appropriate given the nature of the new offence at section 82.3 of sabotage involving a foreign government principal.

408. Subsection 82.13(2) clarifies that the following steps can be taken towards preparing for proceedings, without the written consent of the Attorney-General having been given:

- a person may be arrested for the offence and a warrant for such an arrest may be issued and executed
- a person may be charged with the offence, and
- a person so charged may be remanded in custody or on bail.

409. Given the seriousness of offences contained in Division 82 of the Criminal Code, it is appropriate that some measures towards commencing proceeds be permitted without the consent of the Attorney-General. The steps specified at subsection 82.13(2) are intended to ensure that law enforcement agencies can intervene to prevent a person from continuing to offend, promoting the protection of the Australian public and Australia's national interests.

410. Subsection 82.13(3) provides that nothing in subsection 82.13(2) prevents the discharge of the accused if proceedings are not continued within a reasonable time. Australian common law recognises that a prosecution may be stayed where there is undue delay, to protect Australia's justice system from abuse of processes. The right to stay a prosecution also supports the Court's role in providing procedural fairness to a defendant, and helps maintain public confidence in the administration of justice. It is therefore appropriate that subsection 82.13(3) specify that the steps towards commencing proceedings as described at subsection 82.13(2) do not prevent the discharge of the accused if proceedings are not continued within a reasonable time.

411. Subsection 82.13(4) provides that the Attorney-General must consider whether the conduct constituting an offence against Division 82 of the Criminal Code might be authorised by section 82.10, which provides a defence to offences against Division 82 where:

- the conduct the person engaged in was accessing or using a computer or other electronic system, and
- the person engaged in the conduct in the person's capacity as a public official.

412. In this example, the Attorney-General must consider whether an accused's conduct might be authorised as described in the defence at subsection 82.10 when considering whether to provide consent to prosecute a sabotage offence.

Division 83 – Other threats to security

Section 83.1 – Advocating mutiny

413. Section 83.1 will replace the existing offence of inciting mutiny at section 25 of the Crimes Act, which will be repealed by Item 43 of Schedule 1.

414. Section 83.1 creates an offence that applies where a person advocates mutiny, reckless as to whether the result will be that a defence member takes part in a mutiny.

415. The offence will carry a maximum penalty of seven years imprisonment.

416. An example of this offence is as follows. Person A is an Australian citizen and is married to a member of the Australian Defence Force. Person A is aware that his spouse is unhappy in her role and encourages his spouse to convince other members of the Australian Defence Force to resist orders from their superiors so that a particular Defence operation against one of Australia's enemies cannot take place.

417. This offence is required in addition to the existing offence of incitement (section 11.4 of the Criminal Code) because of the broader definition of the term 'advocates' compared to the definition of incitement. The ancillary offence of incitement means to 'urge' the commission of an offence whereas the term 'advocates' includes promoting and encouraging

an offence. The ancillary offence of incitement also requires the person to intend that the offence incited be committed (subsection 11.4(2) of the Criminal Code) whereas section 83.1 will apply where a person is reckless as to whether the result will be that a defence member will take part in a mutiny. It is appropriate to criminalise this broader range of conduct due to the potentially serious military consequences of the commission of a mutiny offence by a defence force member.

418. To establish this offence, the prosecution will need to prove beyond a reasonable doubt that:

- the person (the advocate) intentionally engages in conduct
- the advocate's conduct involves advocating mutiny and the advocate is reckless as to this element
- the advocate engages in the conduct reckless as to whether the result will be that a defence member (within the meaning of the Defence Force Discipline Act) will take part in a mutiny, and
- at the time he or she engaged in the conduct, the advocate was:
    - was an Australian citizen, and knew that he or she was an Australian citizen
    - was a resident of Australia, and knew that he or she was an Australian citizen
    - had voluntarily put him or herself under the protection of the Commonwealth, and knew that he or she had done so, or
    - was a body corporate incorporated by or under a law of the Commonwealth or of a State or Territory.

419. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 83.1(1)(a). Under section 5.2 of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

420. Recklessness is the fault element for paragraphs 83.1(1)(b) and (c). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and
- a result if he or she is 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 the risk.

421. Knowledge is the fault element for subparagraphs 83.1(1)(d)(i) and (ii). Section 5.3 of the Criminal Code provides that a person has knowledge of a circumstance if he or she is aware that it exists or will exist in the ordinary course of events.

422. Strict liability will apply to subparagraph 83.1(1)(d)(iii) consistent with subsection 83.1(3).

423. For paragraph 83.1(1)(a) of the offence, the prosecution will have to prove beyond a reasonable doubt that the defendant intentionally engaged in the relevant conduct. Consistent with subsection 4.1(2) of the Criminal Code, the reference to 'engages in conduct' in paragraph 83.1(1)(a) means to do an act or to omit to perform an act.

424. For paragraph 83.1(1)(b) of the offence, the prosecution will have to prove beyond a reasonable doubt that the defendant's conduct involves advocating mutiny. The fault element for this element is recklessness. Therefore, the defendant must have been aware of a substantial risk that his or her conduct constituted advocating mutiny, and having regard to the circumstances known to him or her it was unjustifiable to take that risk.

425. The term 'mutiny' is defined at subsection 83.1(2) as a combination between persons who are, or at least two of whom are, members of the Australian Defence Force:

- to overthrow lawful authority in the Australian Defence Force or in a force of another country that is acting in cooperation with the Australian Defence Force, or

- to resist such lawful authority in such a manner as to substantially prejudice the operational efficiency of the Australian Defence Force, or of a part of, a force of another country that is acting in cooperation with the Australian Defence Force.

426. This definition is consistent with the definition of mutiny in section 3 of the Defence Force Discipline Act.

427. The term 'advocate' is not defined and is intended to take its ordinary meaning, including to counsel, promote, encourage or urge the commission of a mutiny. The ordinary meaning of each of the relevant expressions varies, but it is important that they be interpreted broadly to ensure a person who advocates mutiny does not escape punishment by relying on a narrow construction of the terms or one of the terms. However, some examples of the ordinary meaning of each of the expressions follow: to 'counsel' the doing of an act (when used as a verb) is to urge the doing or adoption of the action or to recommend doing the action; to 'encourage' means to inspire or stimulate by assistance or approval; to 'promote' means to advance, further or launch; and 'urge' covers pressing by persuasion or recommendation, insisting on, pushing along and exerting a driving or impelling force.

428. While there may be some overlap between the expressions, it is clear that they do not cover merely commenting on or drawing attention to a factual scenario.

429. For paragraph 83.1(1)(c) the prosecution will have to prove beyond a reasonable doubt that the defendant engaged in the conduct reckless as to whether the result would be that a defence member (within the meaning of the Defence Force Discipline Act) would take part in a mutiny. Therefore, the defendant must have been aware of a substantial risk that his or her conduct would result in a defence member taking part in a mutiny and having regard to the circumstances known to him or her it was unjustifiable to take that risk.

430. Paragraph 83.1(1)(c) specifies that the term 'defence member' takes its meaning from its definition in the Defence Force Discipline Act. The term is defined in section 3 of the Defence Force Discipline Act as:

- a member of the Permanent Navy, the Regular Army or the Permanent Air Force, or
- a member of the Reserves who is:
    - rendering continuous full-time service, or
    - is on duty or in uniform.

431. Section 3 of the Defence Force Discipline Act defines 'Reserves' as meaning the Naval Reserve, the Army Reserve and the Air Force Reserve.

432. Any person, not just a defence member, will be able to commit the offence of advocating mutiny under section 83.1 even though they are not able to commit the primary offence of mutiny that exists at section 20 of the Defence Force Discipline Act. However, in accordance with paragraph 83.1(1)(d), the person will have to have an allegiance to Australia in order to be able to commit the offence.

433. Subsection 20(1) of the Defence Force Discipline Act creates an offence of mutiny (as defined in section 3 of that Act), punishable by a maximum penalty of 10 years imprisonment, where a defence member takes part in a mutiny. Subsection 20(2) creates an offence, punishment by imprisonment for life, where a defence member takes part in a mutiny and the mutiny's object, or one of its objects, is the refusal or avoidance of duty or service in connection with operations against the enemy or the impeding of the performance of such a duty or service.

434. The offence at section 83.1 complements these offences by ensuring that a person who advocates the commission of these serious offences by a defence member is also subject to serious criminal penalties.

435. For subparagraphs 83.1(1)(d)(i) and (ii), the prosecution will have to prove beyond a reasonable that, at the time he or she engaged in the conduct, the person was, and knew that he or she was:

- an Australian citizen (defined in section 2B of the Acts Interpretation Act and section 4 of the Australian Citizenship Act)
- a resident of Australia (defined in the Dictionary to the Criminal Code as an individual who is a resident of Australia), or
- voluntarily under the protection of the Commonwealth (for example through the grant of asylum).

436. Under section 5.3 of the Criminal Code, a person has knowledge of a circumstance if he or she is aware that it exists or that it will exist in the ordinary course of events.

437. For subparagraph 83.1(1)(d)(iii), the prosecution will have to prove that the person is a body corporate incorporated by or under a law of the Commonwealth or of a State or

Territory. Strict liability is appropriate for this element because section 12.3 of the Criminal Code (which provides that where knowledge is a fault element, the element attributed to a body corporate is that they 'expressly, tacitly or impliedly authorised or permitted the commission of the offence') fits well with establishing that the body corporate 'knows' it is incorporated under a law of the Commonwealth.

438. Strict liability is set out in section 6.1 of the Criminal Code. The effect of applying strict liability to an element of an offence means that no fault element needs to be proved and the defence of mistake of fact is available.

439. The defence of mistake of fact is set out in section 9.2 of the Criminal Code. The defence provides that a person is not criminally responsible for an offence that includes a physical element to which strict liability applies if:

- at or before the time of the conduct constituting the physical element, the person considered whether or not a fact existed, and is under a mistaken but reasonable belief about those facts, and

- had those facts existed, the conduct would not have constituted an offence.

440. This offence will only be able to be committed by a person who owes an allegiance to the Commonwealth (paragraph 83.1(1)(d)). The person must know that they owe an allegiance to the Commonwealth. This is appropriate because only persons who benefit from the protection of the Australian state should be penalised for advocating that members of the Australian Defence Force take part in a mutiny.

441. Subsection 83.1(4) applies Section 15.4 (extended geographical jurisdiction—Category D) to the offence at subsection 83.1 (advocating mutiny). Under section 15.4, the effect of Category D geographical jurisdiction is that the offence applies:

- whether or not the conduct constituting the alleged offence occurs in Australia, and

- whether or not a result of the conduct constituting the alleged offence occurs in Australia.

442. Category D jurisdiction is appropriate because the Australian Defence Force engages in conduct that is outside Australian territory and members of the ADF may be vulnerable to a person advocating mutiny while overseas. Consistent with section 83.1(1)(d), only persons who owe an allegiance to Australia will be able to commit the offence, regardless of where the conduct occurs.

443. 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).

444. 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.

Section 83.2 – Assisting prisoners of war to escape

445. Section 83.2 will replace the existing offence of assisting prisoners of war to escape at section 26 of the Crimes Act, which will be repealed by Item 43 of Schedule 1.

446. Section 83.2 creates an offence that applies where a person assists one or more prisoners of war to escape from custody controlled by the Commonwealth or Australian Defence Force in the context of an international armed conflict. The offence will be punishable by a maximum penalty of 15 years imprisonment.

447. An example of this offence is as follows. Australia is engaged in an international armed conflict on the territory of another country. Person A is a detention officer that works in a Commonwealth controlled detention facility in that country. Person A intentionally leaves the facility unlocked overnight so that a number of prisoners of war are able to escape.

448. To establish the offence, prosecution will need to prove beyond reasonable doubt that:

- the person intentionally engages in conduct
- the person's conduct assists one or more prisoners of war (within the meaning of Article 4 of the Third Geneva Convention) to escape from custody and the person is reckless as to this element
- the custody is controlled wholly or partly by the Commonwealth or the Australian Defence Force and the person is reckless as to this element, and
- the conduct takes place in the context of, and is associated with, an international armed conflict.

449. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 83.2(1)(a). Under section 5.2 of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

450. Recklessness is the fault element for paragraphs 83.2(1)(b) and (c). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and
- a result if he or she is 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 the risk.

451. Absolute liability will apply to paragraph 83.2(1)(d) consistent with subsection 83.2(2).

452. For paragraph 83.2(1)(a) of the offence, the prosecution will have to prove beyond a reasonable doubt that the defendant intentionally engaged in the relevant conduct. Consistent with subsection 4.1(2) of the Criminal Code, the reference to 'engages in conduct' in paragraph 83.2(1)(a) means to do an act or to omit to perform an act.

453. For paragraph 83.2(1)(b) of the offence, the prosecution will have to prove beyond a reasonable doubt that the conduct assists one or more prisoners of war (within the meaning of Article 4 of the Third Geneva Convention) to escape from custody. The terms escape and custody are not defined and are intended to take their ordinary meaning.

454. Article 4 of the Third Geneva Convention defines prisoners of war as 'those who, at a given moment and in any manner whatsoever, find themselves, in case of a conflict or occupation, in the hands of persons a Part to the conflict or Occupying Power of which they are nationals'. Prisoners of war are therefore members of the armed forces of one of the parties to a conflict who fall into the hands of the adverse party.

455. The term escape in intended to include a continuum of conduct that could include physically breaking free from a place of detention and other conduct that contributes to a person eluding, avoiding, evading, or breaking free from the custody of the Commonwealth or the Australian Defence Force.

456. The term custody is intended to describe when a person is in the care or control of the Commonwealth or the Australian Defence Force. It is not intended that the term custody be linked to a particular type or location of detention. The term is intended to include custody that could take place in permanent, temporary or itinerant locations, both within and outside of Australian territory.

457. The fault element for paragraph 83.2(1)(b) is recklessness. Therefore, the defendant must have been aware of a substantial risk that his or her conduct assists one or more prisoners of war (within the meaning of Article 4 of the Third Geneva Convention) to escape from custody, and having regard to the circumstances known to him or her it was unjustifiable to take that risk.

458. For paragraph 83.2(1)(c) of the offence, the prosecution will have to prove beyond a reasonable doubt that the custody is controlled wholly or partly by the Commonwealth or the Australian Defence Force. The fault element for this element is recklessness. Therefore, the defendant must have been aware of a substantial risk that the custody is controlled wholly or partly by the Commonwealth or the Australian Defence Force and that, having regard to the circumstances known to him or her it was unjustifiable to take that risk.

459. The term controlled could include financial, administrative or operational power, authority, governance, leadership or command.

460. For paragraph 83.2(1)(d), the prosecution will have to prove beyond a reasonable doubt that the conduct takes place in the context of, and is associated with, an international armed conflict.

461. The term international armed conflict is intended to take its meaning from International Humanitarian Law. Common Article 2 to the Geneva Conventions of 1949 states the Conventions 'shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of

war is not recognized by one of them.' Accordingly, the term international armed conflict in the context of the offence at section 83.2 means armed conflict between two nation States. It is not intended for the term international armed conflict to include conflict with or between non-state actors such as terrorist groups, or conflict within a State, such as in times of civil war or internal disturbance.

462. The terms 'in the context of', and 'associated with' are not defined and are intended to take their ordinary meaning. Both terms are intended to establish a clear connection between the conduct and the circumstance of international armed conflict.

463. Subsection 83.2(2) applies absolute liability to paragraph 83.2(1)(d). Absolute liability is set out in section 6.2 of the Criminal Code. The effect of applying absolute liability to an element of an offence is that no fault element needs to be proved and the defence of mistake of fact is unavailable. Accordingly, prosecution will not be required to prove that the person knew or was reckless as to the fact that the defendant's conduct took place in the context of, and in association with, an international armed conflict.

464. Absolute liability is appropriate and required for the element of the offence that the conduct takes place in the context of, and is associated with, an international armed conflict. This element reflects the circumstances in which Article 4 of the Third Geneva Conventions apply, which is limited to international armed conflict, and does not relate to the substance of the offence.

465. As described above, the prosecution will need to prove that the defendant was aware of a substantial risk that his or her conduct assists one or more prisoners of war to escape from custody that is controlled by the Commonwealth or the Australian Defence Force, and having regard to the circumstances known to him or her it was unjustifiable to take that risk. The issue of whether the person knows that their conduct takes place in the context of, and in association with, an international armed conflict is not relevant to their culpability. This is consistent with Commonwealth criminal law practice, as described in the Guide to Framing Commonwealth Offences.

466. The application of absolute liability to paragraph 83.2(1)(d) also ensures that a person cannot avoid criminal responsibility because they were unaware of the type of conflict that gave rise to the circumstance of the Commonwealth or Australian Defence Force having custody of one or more prisoners of war. With the application of absolute liability, a defendant could, for example, admit that they knew they were assisting a prisoner of war to escape from the custody of the Commonwealth or Australian Defence Force, but thought that they had done so in the context of non-international armed conflict, rather than an international armed conflict.

467. Subsection 83.2(3) applies Section 15.4 (extended geographical jurisdiction—Category D) to section 83.2. Under section 15.4, the effect of Category D geographical jurisdiction is that the offence applies:

- whether or not the conduct constituting the alleged offence occurs in Australia, and
- whether or not a result of the conduct constituting the alleged offence occurs in Australia.

468. Category D jurisdiction is appropriate in order to cover offences that occur within the context of international armed conflicts that do not take place within Australian territory, for example, when Australia is taking part in military operations overseas. It is foreseeable that the Australian Defence Force would have custody of prisoners of war (within the meaning of Article 4 of the Third Geneva Convention) wholly outside of Australia. This offence needs to criminalise conduct that assists such prisoners of war to escape.

469. 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.

Section 83.3 – Military-style training involving foreign government principal

470. Section 83.3 creates an offence that applies where a person provides, receives or participates in training that involves using arms or practising military exercises, movements or evolutions. The offence applies when that training is provided on behalf of a foreign government principal, or is directed, funded or supervised by a foreign government. Appropriate defences apply to permit training expressly authorised by the Commonwealth, as part of service with the armed forces of the government of a foreign country, or where a declaration in relation to specified armed forces is made. The offence is punishable by a maximum penalty of 20 years imprisonment.

471. An example of this offence is as follows. Person A participates in training in Australia which is provided by Country E. The training involves the use of weapons and military-style drills. Country E is undertaking the training at a hidden rural location and intends for the training to assist it to conduct military operations against Country F, a close neighbour of Australia. Person A is intending to participate in those future military operations against Country F.

472. To establish this offence, the prosecution will need to prove beyond a reasonable doubt that:

- the person intentionally provides, receives, or participates in, training
- the training involves using arms or practising military exercises, movements or evolutions and the person is reckless as to this element, and
- the training is provided on behalf of a foreign government principal, or is directed, funded or supervised by a foreign government principal and the person is reckless as to this element.

473. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 83.3(1)(a). Under section 5.2 of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

474. Recklessness is the fault element for paragraphs 83.3(1)(b) and (c). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and

- a result if he or she is 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 the risk.

475. For paragraph 83.3(1)(a) of the offence, the prosecution will have to prove beyond a reasonable doubt that the defendant intentionally provides, receives or participates in training. The terms provides, receives and participates are not defined and are intended to take their ordinary meanings.

476. The term 'provides' could include organising, facilitating, supplying, and delivering training. The term is intended to include any conduct that actually constitutes the delivery of the content of the training. However, it could also include conduct that contributes to the provision of training, such as supplying weapons or constructing the training course.

477. The terms 'receives' and 'participates' could include being given or accepting, taking part in, engaging in, joining, being involved in and partaking in training. The terms are intended to cover situations where a person only received or participates in part of the training. For example, Person A might engage in just one day of a ten day training course of the type described in subsection 83.3(1).

478. The term 'training' could include instruction, tuition, preparation, guidance, lessons, drilling and priming.

479. The prosecution will have to prove beyond a reasonable doubt that the training involves using arms or practising military exercises, movements or evolutions. The fault element for this element is recklessness. Therefore, the defendant must have been aware of a substantial risk that his or her conduct involves the use of arms or practising military exercises, movements or evolutions and, having regard to the circumstances known to him or her it is not justifiable to take that risk.

480. The terms 'using', 'arms', 'practising' and 'military exercises, movements or evolutions' are not defined and are intended to take their ordinary meanings.

481. The term 'use of' could include to take hold of, deploy, operate, wield and handle.

482. The term 'arms' is intended to include any instrument or instrumentality used to inflict bodily harm or physical damage. The term is intended to be interpreted broadly and could include items that were not originally designed for the purpose of being used as arms. Examples of arms could include:

- items with blades including knives, machetes, axes and spears

- items with ammunition including guns and rifles

- items with explosive capability including land mines, bombs and grenades

- items that disperse hazardous substances such as hazardous gas, and

- items repurposed as arms, for example tools, sports equipment, construction materials and objects made of glass.

483. The term 'practising' could include rehearsing, working at, working on and running through. This term is intended to include conduct that involves physical activity such as practising military drills, and non-physical activity such as studying or learning about the use of arms, military exercises, movements or evolutions.

484. The term 'military exercises, movements or evolutions' is intended to include activities that involve the use of military resources in training for military purposes. This could include activities to increase capabilities in operations, combat or strategy. The term 'military' is not intended to restrict the exercises, movements or evolutions to those conducted by State armed forces. The term is intended to relate to the character of the 'exercises, movements or evolutions' in that they involve the use of arms and are organised and coordinated in their delivery. The term 'evolutions' is intended to capture military manoeuvres involving planned and regulated movements of troops or tactical exercises carried out in the field.

485. The prosecution will have to prove beyond a reasonable doubt that the training is provided on behalf of a foreign government principal, or is directed, funded or supervised by a foreign government principal. The fault element for this element is recklessness. Therefore, the defendant must have been aware of a substantial risk that the circumstances described at paragraph 83.3(1)(c) exist, and having regard to the circumstance known to him or her it was unjustifiable to take that risk.

486. The terms 'on behalf of', and 'directed', 'funded' and 'supervised' are not defined and are intended to take their ordinary meanings.

487. Subparagraph 83.3(1)(c)(i) provides that 'foreign government principal' has the meaning given to it by Part 5.2 of the Criminal Code, and is defined at section 90.3.

488. Section 90.3 provides that each of the following is a ***foreign government principal***:

- the government of a foreign country or a part of a foreign country
- an authority of the government of a foreign country
- an authority of the government of part of a foreign country
- a foreign local government body or foreign regional government body
- a company to which any of the subparagraphs of paragraph (a) of the definition of foreign public enterprise in section 70.1 applies
- a body or association to which either of the subparagraphs of paragraph (b) of the definition of foreign public enterprise in section 70.1 applies
- a foreign political organisation, or

- an entity or organisation directed or controlled:
    - by a foreign government principal within the meaning of any other paragraph of this definition, or
    - by two or more such foreign government principals that are foreign government principals of the same foreign country.

489. Paragraphs (a) to (d) of this definition cover governments or authorities of foreign countries. ***Foreign country*** is defined in the Dictionary to the Criminal Code as including:

- a colony or overseas territory
- a territory outside Australia, where a foreign country is to any extent responsible for the international relations of the territory, and
- a territory outside Australia that is to some extent self-governing, but that is not recognised as an independent sovereign state by Australia.

490. For subparagraph 83.3(1)(c)(i), the term 'on behalf of' is intended to include where a person or entity represents, acts in the interests of, or acts as a proxy for, a foreign government principal.

491. For subparagraph 83.3(1)(c)(ii), the term 'directed' and 'supervised' could include controlled, managed, governed, instructed, administered, overseen, presided over and run. The term is intended to include where the direction or supervision is in part or in whole. For example, a foreign government principal might instruct that training be conducted, but the details of that training are overseen by a subcontracted company that delivers the training.

492. For subparagraph 83.3(1)(c)(ii), the term 'funded' is intended to include when a foreign government principal or person acting on behalf of a foreign government principal provides resources towards the training described in subsection 83.3(1). The term is intended to include where the funding is in part or in whole. The term is also intended to include financing, loans, agreements, appropriations, contracts or promises of funding, in part or in whole.

493. It is possible that a defendant will know, or be reckless, as to the fact that they are providing, receiving or participating in training that is provided by, directed, funded or supervised by a person who identifies himself or herself as an official of a foreign government. In this case, the person will be engaging in the conduct on behalf of the foreign principal and the defendant will have satisfied the elements of the offence as described at subparagraph 83.3(1)(c).

494. However, it may also be the case that the defendant provides, receives or participates in training that is provided by, directed, funded or supervised by an intermediary, and not by a foreign government principal, or foreign government official. In this case, the prosecution will have to prove beyond a reasonable doubt that the defendant was aware of a substantial risk that he or she was engaging in training provided on behalf of, directed, funded or supervised by a person acting on behalf of a foreign principal and that it was unjustifiable to take that risk. This may be the case where, for example, the intermediary advises the

defendant that the intermediary acts in coordination with foreign officials, or the intermediary facilitates preferential treatment for the defendant from a foreign government.

495. 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.

496. Subsection 83.3(2) provides that the offence created by subsection 83.3(1) does not apply to a person in relation to conduct engaged in by the person that is authorised by written agreement to which the Commonwealth is a party. The term 'written agreement' could include agreement through a memorandum of understanding, diplomatic correspondence, the exchange of letters or emails, or an international instrument. The term 'Commonwealth' is intended to include Commonwealth entities including Commonwealth departments and agencies.

497. An example of where the defence at subsection 83.3(2) could apply is where members of the Australian Defence Force are permitted through a memorandum of understanding to undertake training of the kind described at subsection 83.3(1) with the military forces of a foreign government.

498. The Note under subsection 83.3(2) notes that the defendant will bear an evidential burden in relation to the defence at subsection 83.3(2). Consistent with section 13.3 of the Criminal Code, the defendant will need to point to evidence that suggests a reasonable possibility that the defence is made out. If this is done, the prosecution must refute the defence beyond reasonable doubt.

499. It is appropriate that the defendant bear the evidential burden in relation to this defence as they are best placed to know of the existence of the type of agreement described at subsection 83.3(2) and to produce evidence in relation to that agreement.

500. Subsection 83.3(3) provides that the offence created by subsection 83.3(1) does not apply in relation to training in the course of, or as part of a person's service with:

- the armed forces of the government of a foreign country, or
- any other armed force if a declaration under subsection 119.8(1) covers the person and the circumstances of the person's service in or with the armed force.

501. For paragraph 83.3(3)(a), it is appropriate that a defence be available to a person in the course of, and as part of, a person's service with the armed forces of the government of a foreign country. For example, a person may be required to undertake compulsory military service with the armed forces of the government of a foreign country of which they are a citizen. In this example, the defence at paragraph 83.3(3)(a) would be available.

502. The defendant will bear an evidential burden in relation to the defence at paragraph 83.3(3)(a). Consistent with section 13.3 of the Criminal Code, the defendant will

need to point to evidence that suggests a reasonable possibility that the defence is made out. If this is done, the prosecution must refute the defence beyond reasonable doubt.

503. In relation to paragraph 83.3(3)(b), subsection 119.8(1) of the Criminal Code provides that the Minister may by legislative instrument make a declaration concerning a specified person or class of persons. To make such a declaration, the Minister must be satisfied that it is in the interests of the defence or international relations of Australia to permit service with a specified armed force in a foreign country.

504. An example of when a declaration might be made under subsection 119.8(1) could include where an individual is providing training assistance on behalf of a foreign government with the consent of both the Australian and foreign governments.

505. The defendant will bear an evidential burden in relation to the defence at paragraph 83.3(3)(b). Consistent with section 13.3 of the Criminal Code, the defendant will need to point to evidence that suggests a reasonable possibility that the defence is made out. If this is done, the prosecution must refute the defence beyond reasonable doubt.

506. Subsection 83.3(4) specifies that subsection 83.3(3) does not apply if at the time of engaging in the conduct described at 83.3(1), the person is:

- in or with a listed terrorist organisation within the meaning at Part 5.3 or a prescribed organisation within the meaning of Part 5.5, or

- the training is wholly or partly funded by a listed terrorist organisation within the meaning at Part 5.3 or a prescribed organisation within the meaning of Part 5.5.

507. Part 5.3 of the Criminal Code defines 'listed terrorist organisation' as an organisation that is specified by regulations for the purposes of paragraph (b) of the definition of 'terrorist organisation' in section 102.1.

508. Part 5.5 of the Criminal Code defines 'prescribed organisation' as an organisation prescribed by the regulations for the purpose of this paragraph, or an organisation referred to paragraph (b) of the definition of 'terrorist organisation' in subsection 102.1(1).

509. Subsection 83.3(4) is appropriate to ensure the offence is consistent with, and complements, Commonwealth terrorism offences at Division 101 of the Criminal Code. Subsection 83.3(4) also guards against situations where the armed forces of a foreign country, or a foreign country's government, itself is listed terrorist or other prescribed organisations.

510. Subsection 83.3(5) applies Section 15.2 of the Criminal Code (extended geographical jurisdiction – Category B) to section 83.3. Under section 15.2, the effect of Category B jurisdiction is that the offence applies:

- if the conduct constituting the offence occurs wholly or partly in Australia

- if the result of that conduct occurs wholly or partly in Australia, and

- if the conduct occurs outside Australia and at the time of committing the offence, the person is an Australian citizen, resident or body corporate.

511. Category B jurisdiction is appropriate to ensure that this offence appropriately protects Australia's from military threats caused by unlawful military training undertaken on behalf of a foreign government principal, wherever that conduct occurs.

Section 83.4 – Interference with political rights and duties

512. Section 83.4 will replace the existing offence of interfering with political liberty at section 28 of the Crimes Act, which will be repealed by Item 43 of Schedule 1.

513. Section 83.4 creates an offence that applies where a person uses force, violence, threats or intimidation to interfere with a person's democratic or political right under the Constitution or Commonwealth law.

514. The offence will be punishable by a maximum penalty of ten years imprisonment.

515. An example of this offence is where Person C wishes to prevent Person D from exercising their right to vote because Person C knows that Person D is going to vote for a particular Senate candidate in a federal election. Person C considers the relevant candidate unfit to hold public office because of their extreme views. Person C threatens to cause serious physical harm to Person D if they vote for that particular candidate in the election.

516. To establish the offence, prosecution will need to prove beyond reasonable doubt that:

- the person intentionally engages in conduct
- the person's conduct involves:
    - the use of force
    - violence
    - intimidation, or
    - the making of threats of any kind

  and the person is reckless as to this element
- the person's conduct will result in interference with the exercise or performance, by another person, of an Australian democratic or political right and the person is reckless to this element, and
- the right arises under the Constitution or a law of the Commonwealth.

517. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 83.4(1)(a). Under section 5.2 of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

518. Recklessness is the fault element applying to paragraphs 83.4(1)(b) and (c). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and

- a result if he or she is 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.

519. Absolute liability will apply to the circumstance in paragraph 83.5(1)(d) consistent with subsection 83.4(2).

520. For paragraph 83.4(1)(a) of the offence, the prosecution will have to prove beyond a reasonable doubt that the defendant intentionally engaged in the relevant conduct. Consistent with subsection 4.1(2) of the Criminal Code, the reference to 'engages in conduct' in paragraph 83.4(1)(a) means to do an act or to omit to perform an act.

521. While it is unlikely that an omission could constitute force, violence, intimidation or threats, the term 'engages in conduct' allows the prosecution to allege a course of conduct in charging an offence rather than being required to identify a particular act as constituting the offending conduct.

522. For paragraph 83.4(1)(b) of the offence, the prosecution will have to prove beyond a reasonable doubt that the person's conduct involves the use of force or violence, or intimidation, or the making of threats of any kind. The fault element for this element is recklessness. Therefore, the defendant must have been aware of a substantial risk that his or her conduct involves force, violence, intimidation or threats and, having regard to the circumstances known to him or her it was unjustifiable to take that risk.

523. The terms force, violence and intimidation are not defined and are intended to take their ordinary meanings.

- The term *force* could include acts such as restraining, manipulating, coercing and physically making a person do something against their will.

- The term *violence* is not intended to require evidence of actual harm to establish that an act of violence has been conducted. For example, a person might set off an explosive device to interfere with a political protest, but the device does not actually cause harm to any person. For the purposes of paragraph 83.4(1)(b), it is intended that this conduct would be considered an act of violence and would satisfy this element of the offence.

- The term *intimidation* is intended to include conduct that makes a person timid or fearful.

- The term ***threat*** is defined in the Dictionary to the Criminal Code as including a threat made by any conduct, whether express or implied and whether conditional or unconditional.

524. For paragraph 83.4(1)(c) of the offence, the prosecution will have to prove beyond a reasonable doubt that the person's conduct results in interference with the exercise or performance, by any other person, of an Australian democratic or political right. Recklessness is the fault element for this offence. Therefore, the defendant must have been aware of a substantial risk that his or conduct would result in interference with the exercise or performance, by any other person, of an Australian democratic or political right and, having regard to the circumstances known to him or her it was unjustifiable to take that risk.

525. The term Australian democratic or political right is intended to cover a broad range of rights held by Australians in relation to participation in Australia's democracy, including voting in elections and referenda and participating in lawful protests. The limitation to 'Australian' democratic and political rights is intended to limit the operation of this paragraph only to rights that arise because of a person's status as Australian. For example, it is not intended to cover a situation where a person is a joint citizen of Australia and the United Kingdom and has a right to vote in United Kingdom elections while physically located in Australia. This would be a United Kingdom democratic right, rather than an Australian democratic right, even though it is being exercised 'in' Australia.

526. For paragraph 83.4(1)(d) of the offence, the prosecution will have to prove beyond reasonable doubt that the democratic or political right referred to in paragraph 83.4(1)(c) arises under the Constitution or a law of the Commonwealth. This paragraph ties the offence to Commonwealth jurisdiction. For example, interference with democratic and political rights arising under state and territory law would not captured by this offence. Examples of democratic and political rights under the Constitution or a law of the Commonwealth include:

- the right to vote
- the implied right to freedom of political communication
- making political donations

527. Subsection 83.4(2) applies absolute liability to paragraph 83.4(1)(d). Absolute liability is set out in section 6.2 of the Criminal Code. The effect of applying absolute liability to an element of an offence is that no fault element needs to be proved and the defence of mistake of fact is unavailable. Accordingly, for paragraph 83.4(1)(d), the prosecution will be required to prove only the physical element that the Australian democratic and political right 'arises under the Constitution or a law of the Commonwealth.'

528. Absolute liability is appropriate and required for the element of the offence that the right arises under the Constitution or a law of the Commonwealth because this element is a jurisdictional element of the offence. A jurisdictional element of the offence is an element that does not relate to the substance of the offence, but marks a jurisdictional boundary between matters that fall within the legislative power of the Commonwealth and those that do not. The issue of whether the person knew that the right arose under the Constitution or a law of the Commonwealth is not relevant to their culpability. This is consistent with Commonwealth criminal law practice, as described in the Guide to Framing Commonwealth Offences.

529. The application of absolute liability to paragraph 83.4(1)(d) also ensures that a person cannot avoid criminal responsibility because they were unaware of the level of government law that gave rise to a particular Australian democratic or political right, for example by

admitting that they knew they were interfering with the exercise by another person of an Australian democratic or political right but thought that the right arose due to a law of a State rather than a law of the Commonwealth.

530. The Note to subsection 83.4(1) clarifies that the defence for acts of done in good faith at subsection 80.3 applies to the offence at section 83.4.

531. An example of where the defence at section 80.3 could apply is where a person participates in a counter-protest and forcefully and aggressively shouts at the opposing protestors in an intimidating way, but does so in order to point out, in good faith, the errors in the arguments or position of the opposing protestors.

532. The defendant will bear an evidential burden in relation to the defence at section 80.3 in relation to acts done in good faith. It is appropriate for the defendant to bear an evidential burden because the defendant is placed to explain their motivations when engaging in the relevant conduct and it is peculiarly within their knowledge as to how and why they should be considered to be acting in good faith. Section 13.3 of the Criminal Code provides that in the case of a standard 'evidential burden' defence, the defendant bears the burden of pointing to evidence that suggests a reasonable possibility that the defence is made out. If this is done, the prosecution must refute the defence beyond reasonable doubt (section 13.1).

533. 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.

Section 83.5 – Consent of Attorney-General required for prosecutions

534. Section 83.5 requires the written consent of the Attorney-General to commence proceedings against a person for offences in Division 83 of the Criminal Code, and is intended to ensure that there is appropriate oversight of prosecutions. This is appropriate given the nature of the offences in Division 83 and the potential for national security or international considerations to arise.

535. 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 CDPP is not able to take into account under the *Prosecution Policy of the Commonwealth*.

536. Section 83.5 provides the Attorney-General with an opportunity to receive advice from relevant agencies and other Ministers about sensitivities that might arise if proceedings are commenced for offences under Division 83, and provides opportunity for consideration of whether the prosecution could be detrimental to Australia's foreign relations and national security.

537. Subsection 83.5(2) clarifies that the following steps can be taken towards preparing for proceedings, without the written consent of the Attorney-General having been given:

- a person may be arrested for the offence and a warrant for such an arrest may be issued and executed
- a person may be charged with the offence, and

- a person so charged may be remanded in custody or on bail.

538. Given the seriousness of offences contained in Division 83 of the Criminal Code, it is appropriate that some measures towards commencing proceeds be permitted without the consent of the Attorney-General. The steps specified at subsection 83.5(2) are intended to ensure that law enforcement agencies can intervene to prevent a person from continuing to offend, promoting the protection of the Australian public and Australia's national interests.

539. Subsection 83.5(3) provides that nothing in subsection 83.5(2) prevents the discharge of the accused if proceedings are not continued within a reasonable time. Australian common law recognises that a prosecution may be stayed where there is undue delay, to protect Australia's justice system from abuse of processes. The right to stay a prosecution also supports the Court's role in providing procedural fairness to a defendant, and helps maintain public confidence in the administration of justice. It is therefore appropriate that subsection 83.5(3) specify that the steps towards commencing proceedings as described at subsection 83.5(2) do not prevent the discharge of the accused if proceedings are not continued within a reasonable time.

540. Subsection 83.5(4) provides that the Attorney-General must consider whether the conduct constituting an offence against Division 83 of the Criminal Code might be authorised by subsections 83.3(2) or (3), which provides defences to an offence against section 83.3, or section 80.3, which provides a defence to an offence against section 83.4.

Item 9

541. Item 9 repeals the heading of Part 5.2 and substitutes a new heading. The heading is changing from 'Offences relating to espionage and similar activities to 'Espionage and related offences. The heading requires updating to reflect the broader range of offences that will be housed within Part 5.2 due to the enactment of new foreign interference offences.

Item 10

<u>Section 90.1 – Definitions</u>

542. Item 10 inserts the following new definitions relevant to the espionage offences into section 90.1 of the Criminal Code:

- deals
- foreign government principal
- foreign political organisation, and
- foreign principal.

543. Section 90.1 defines ***deals*** for the purposes of the espionage offences in Part 5.2. A person ***deals*** with information or an article if the person does any of the following in relation to the information or article:

- receives or obtains it

- collects it
- possesses it
- makes a record of it
- copies it
- alters it
- conceals it
- communicates it
- publishes it, or
- makes it available.

544. Descriptions of what these terms are intended to cover and examples of the types of conduct that would fall within each term are as follows.

- *Receives* is intended to cover being given or presented with information or an article. This would include a person being given a classified document by another person.

- *Obtains* is intended to cover getting or acquiring information or an article. This is intended to be a more active term than 'receives' and implies that a person made an active effort to acquire information or an article. This may include a person opening a filing cabinet or accessing an electronic filing system to get or acquire a document or article.

- *Possesses* is intended to cover a person intentionally exercising control over information or an article. This would include a person having actual physical custody of information or an article, such as having a classified document in their direct custody by storing it in their house or carrying it in their bag. The term is also intended to cover the concept of 'constructive possession' where the person has the ability to control the object even if they have no physical contact with it. An example of this would be where the person has removed a classified document from his or her workplace and secured it in a bank safety deposit box. Although the bank may technically have physical custody of the document, the fact that the person placed the document there and holds the key to the safety deposit box would be sufficient for the person to be 'possessing' the document.

- *Makes a record of it* is intended to cover the situation where a makes notes of the content of classified document. The notes would convey the content of the information but the person would not actually be dealing with the classified document by other than reading it. The notes of the content would be a 'record' of the information for the purposes of this definition.

- *Copies* is intended to cover reproducing or making an identical version of information or an article. The most obvious example of this would be where a person photocopies a classified document and makes an identical copy of the document. It may also include where a person copies the information by making notes that entirely replicate the content of a document. This overlaps with the definition of 'makes a record' to some extent, but 'copies' is intended to cover the situation where the content is replicated entirely whereas a person may 'make a record' of information by making notes that summarise or paraphrase the information.

- *Alters* is intended to cover the situation where a person amends or changes the information or article in any way. This may include amending a classified document to change or remove the classification level, extracting excerpts from a classified document to create a new document, or substituting text to remove recognisable details without losing the essential information.

- *Conceals* is intended to cover hiding or preventing from being seen. This would include a person hiding documents by sliding them between the pages of books or putting them in the bottom of boxes holding other household items that prevent the documents from being seen.

- *Communicates* is intended to cover any actions that disclose, divulge, convey, impart, relay, convey, transmit or pass on information or an article. This would include a person passing a document to another person, whether in person or via electronic means. It would also include a person having a conversation with another person and telling them the information.

- *Publishes* is intended to cover conduct that makes information or an article generally known. For example, a person would 'publish' information for the purpose of these offences if they made information available online. By contrast to 'communicates' or 'makes available', the term 'publishes' implies that the information is made available to a number of people at the same time, as opposed to being disclosed or conveyed in a more direct form to another person.

- *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.

545. Section 90.1 provides that ***foreign government principal*** has the meaning given to it by section 90.3. This term is used in the definition of ***foreign principal*** in section 90.2 (to be inserted by Item 16) and in Division 92A, which creates a new theft of trade secrets offence.

546. ***Foreign political organisation*** is defined to mean a foreign political party or a foreign political organisation. This will include political parties of foreign countries.

547. Section 90.1 provides that ***foreign principal*** has the meaning given to it by section 90.2. This term is used throughout Part 5.2 for the purpose of the espionage and foreign interference offences.

Item 11

548. Item 11 repeals the definition of ***intelligence or security agency*** from section 90.1 of the Criminal Code. This term is not used in the new espionage offences inserted into Part 5.2 of the Criminal Code by Item 16 and is therefore obsolete.

Item 12

549. Item 12 inserts the following new definitions relevant to the espionage offences into section 90.1 of the Criminal Code:

- national security, and
- security classification

550. Section 90.1 provides that ***national security*** has the meaning given to it by section 90.4. This term is used throughout Part 5.2 and also supports the sabotage offences in Division 82.

551. Section 90.1 provides that ***security classification*** has the meaning given to it by section 90.5. This term is used in the espionage offences in Part 5.2 and the secrecy offences in Schedule 2.

Item 13

552. Item 13 repeals the existing definition of ***security or defence*** from section 90.1 of the Criminal Code. This term is not used in the new espionage offences inserted into Part 5.2 of the Criminal Code by Item 16 and is therefore obsolete.

Item 14

553. Item 14 repeals the definition of ***the Commonwealth*** from section 90.1 of the Criminal Code. This term is not relevant for the new espionage offences inserted into Part 5.2 of the Criminal Code by Item 16 and is therefore obsolete.

Item 15

554. Item 15 repeals existing subsections 90.1(2) and (3) and inserts new subsection 90.2(2). Existing subsection 90.1(2) provides that, for Part 5.2, unless the contrary intention appears:

- expressions referring to obtaining, recording, using, having in possession, communicating or retaining including obtaining, recording, using, having in possession, communicating or retaining in whole or in part, and whether the article or information itself, or only the substance, effect or description of the

article or information, is obtained, recorded, used, possessed, communicated or retained, and

- a reference to a sketch, document or article or to information is to be read as including a reference to a copy of, a part of or a copy of a part of a sketch, document or article or information.

555. This provision can be simplified due to the new definition of ***deals***, to be inserted in section 90.1 by Item 10. Item 15 inserts a new subsection 90.1(2), which provides that in Part 5.2, dealing with information or an article includes:

- dealing with all or part of the information or article, and
- dealing only with the substance, effect or description or article.

556. An example of this would be where Person X describes an aspect of a military capability that allows it to effectively countered by a foreign adversary, but does not describe the capability as a whole.

557. Existing subsection 90.1(3) provides that, for the purposes of Part 5.2 of the Criminal Code, a place that is occupied by, or a thing that is under the control of, the Commonwealth is taken to belong to the Commonwealth. This provision is not necessary for the new espionage offences inserted by Schedule 1, and is therefore being repealed by Item 15.

Item 16

558. Item 16 inserts the following new definitions relevant to the espionage offences into section 90.1 of the Criminal Code:

- foreign principal
- foreign government principal,
- national security, and
- security classification

Section 90.2 – Definition of ***foreign principal***

559. Section 90.2 defines ***foreign principal*** as each of the following:

- a foreign government principal
- a public international organisation within the meaning of Division 70 (see section 70.1)
- a terrorist organisation within the meaning of Division 102 (see section 102.1)
- an entity or organisation directed or controlled by:
    - a public international organisation

- a terrorist organisation within the meaning of Division 102

- an entity or organisation directed or controlled by two or more foreign principals within the meaning of any other paragraph of the definition.

560. The term ***foreign government principal*** in paragraph 90.2(a) is further defined at section 90.3, described in detail below.

561. The term ***public international organisation*** in paragraph 90.2(b) refers to the definition in section 70.1 of the Criminal Code. The term public international organisation is defined in section 70.1 of the Criminal Code to mean:

- an organisation:

  - of which two or more countries, or the governments of two or more countries, are members, or

  - that is constituted by persons representing two or more countries, or representing the governments of two or more countries, or

- an organisation established by, or a group of organisations constituted by:

  - organisations of which two or more countries, or the governments of two or more countries, are members, or

  - organisations that are constituted by the representatives of two or more countries, or the governments of two or more countries, or

- an organisation that is:

  - an organ of, or office within, an organisation described above

  - a commission, council or other body established by an organisation so described or such an organ, or

  - a committee, or sub-committee of a committee, of an organisation described above, or of such an organ, council or body.

562. 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.

563. The term terrorist organisation within the meaning of Division 102 of the Criminal Code in paragraph (c) of the definition refers to the definition in section102.1 of the Criminal Code.

564. Section 102.1 of the Criminal Code defines ***terrorist organisation*** to mean:

- an organisation that is directly or indirectly engaged in, preparing, planning, assisting in or fostering the doing of a terrorist act, or
- an organisation that is specified by the regulations.

565. It is appropriate to cover terrorist organisations within the definition of foreign principal because of the significant consequences for Australia's security an offence against Part 5.2 be committed by a person acting on behalf of a terrorist organisation.

566. Paragraph 90.2(e) covers entities or organisations directed or controlled by a public international organisation or a terrorist organisation within the meaning of Division 102. This ensures that foreign principals cannot avoid falling within the definition by using another entity or organisation to undertake espionage or foreign interference activities.

567. Paragraph 90.2(e) covers entities or organisations directed or controlled by two or more foreign principals within the meaning of paragraphs 90.2(a), (b) or (c). For example, two foreign countries with shared interests may jointly establish and control a company which is used to conceal espionage activities against Australia. Paragraph 90.2(e) ensures that such entities fall within the definition of foreign principal.

Section 90.3 – Definition of *foreign government principal*

568. Section 90.3 defines ***foreign government principal*** for the purposes of Part 5.2 of the Criminal Code. This term is used in the definition of ***foreign principal*** in section 90.2 and in the offence in Division 92A regarding theft of trade secrets.

569. Section 90.3 provides that each of the following is a ***foreign government principal***:

- the government of a foreign country or a part of a foreign country
- an authority of the government of a foreign country
- an authority of the government of part of a foreign country
- a foreign local government body or foreign regional government body
- a company to which any of the subparagraphs of paragraph (a) of the definition of foreign public enterprise in section 70.1 applies
- a body or association to which either of the subparagraphs of paragraph (b) of the definition of foreign public enterprise in section 70.1 applies
- a foreign political organisation, or
- an entity or organisation directed or controlled:
    - by a foreign government principal within the meaning of any other paragraph of this definition, or

- by two or more such foreign government principals that are foreign government principals of the same foreign country.

570. Paragraphs 90.3(a) to (d) cover governments or authorities of foreign countries. ***Foreign country*** is defined in the Dictionary to the Criminal Code as including:

- a colony or overseas territory
- a territory outside Australia, where a foreign country is to any extent responsible for the international relations of the territory, and
- a territory outside Australia that is to some extent self-governing, but that is not recognised as an independent sovereign state by Australia.

571. Paragraphs 90.3(a) to (d) ensure that the definition of ***foreign government principal*** comprehensively covers the governments and authorities of foreign countries. Historically, foreign countries are the most likely to seek to engage in espionage and foreign interference activities and it is essential that their activities are covered by the definition regardless of which level of government, or which type of government department or agency, is responsible for the conduct.

572. Under paragraph 90.3(e) of ***foreign government principal***, a company will fall within the definition if any of the subparagraphs of paragraph (a) of the definition of ***foreign public enterprise*** in section 70.1 applies. Paragraph (a) of the definition of ***foreign public enterprise*** means a company where one of the following applies:

- the government of a foreign country or of part of a foreign country holds more than 50% of the issued share capital of the company
- the government of a foreign country or of part of a foreign country holds more than 50% of the voting power in the country
- the government of a foreign country or of part of a foreign country is in a position to appoint more than 50% of the company's board of directors
- the directors (however described) of the company are accustomed or under an obligation (whether formal or informal) to act in accordance with the directions, instructions or wishes of the government of a foreign country or of part of a foreign country, or
- the government of a foreign country or of part of a foreign country is in a position to exercise control over the company.

573. Under paragraph 90.3(f) of the definition of ***foreign government principal***, a company will fall within the definition if either of the subparagraphs of paragraph (b) of the definition of ***foreign public enterprise*** in section 70.1 applies. Paragraph (b) of the definition of ***foreign public enterprise*** means a body or association (other than a company, which is covered by paragraph (a) of the definition in section 70.1) where one of the following applies:

- the members of the executive committee (however described) of the body or association are accustomed or under an obligation (whether formal or

informal) to act in accordance with the directions, instructions or wishes of the government of a foreign country or of part of a foreign country, or

- the government of a foreign country or of part of a foreign country is in a position to exercise control over the body or association.

574. Paragraphs (a) and (b) of the definition of ***foreign public enterprise*** cover state-owned enterprises and other bodies and associations that are controlled by foreign governments. It is essential that these bodies are covered by the definition of ***foreign government principal*** so that there are no gaps in the espionage and foreign interference offences that could be exploited by foreign governments.

575. Paragraph 90.3(g) covers foreign political organisations. ***Foreign political organisation*** is defined by section 90.1 as including foreign political parties. This will include political parties of foreign countries.

576. Paragraph 90.3(h) covers an entity or organisation directed or controlled:

- by a foreign government principal within the meaning of any other paragraph of this definition, or

- by two or more such government principals that are foreign government principals of the same foreign country.

577. Paragraph 90.3(h) ensures that foreign government principals are not able to avoid the application of the espionage and foreign interference activities by channelling their activities through another organisation that is a front for the foreign government principal.

578. Paragraph 90.3(h) also ensures that entities or organisations directed or controlled by more than one foreign government principals (from the same foreign country) are covered by the definition. For example, two authorities of a foreign country may jointly establish an entity and use that organisation to direct espionage in Australia. In this respect, paragraph (h) is limited to situations where the two (or more) foreign government principals are from the same foreign country. This is because entities or organisations that are directed or controlled by more than one foreign country fall within paragraph 90.2(f) of the definition of ***foreign principal***.

Section 90.4 – Definition of ***national security***

579. Section 90.4 provides that the national security of Australia or a foreign country means:

- the defence of the country

- the protection of the country or any part of it, or the people of the country or any part of it, from activities covered by subsection 90.4(2)

- the protection of the integrity of the country's territory and borders from serious threats

- the carrying out of the country's responsibilities to any other country in relation to the protection of the integrity of the country's territory and borders from serious threats and the activities covered by subsection 90.4(2), and

- the country's political, military or economic relations with another country or other countries.

580. Subsection 90.4(2) provides that, for the purposes of subsection 90.4(1), this subsection covers the following activities relating to a country, whether or not directed from, or committed within, the country:

- espionage

- sabotage

- terrorism

- political violence

- activities intended and likely to obstruct, hinder or interfere with the performance by the country's defence force of its functions or with the carrying out of other activities by or for the country for the purposes of its defence or safety, and

- foreign interference.

581. The purpose of the definition of ***national security*** is to exhaustively cover the matters relevant to the security and defence of a country. The definition needs to cover matters relevant to Australia's national security as well as the national security of a foreign country. This is due to the use of this defined term in the espionage offences where a person commits the offence if they intend to prejudice Australia's national security or advantage the national security of a foreign country.

582. This definition reflects traditional concepts of national security that fall within the Commonwealth's legislative power. This includes matters relating to the defence of a country from hostilities and military threats (paragraph 90.4(1)(a)) as well as the protection of a country from espionage, sabotage, terrorism, political violence and foreign interference, whether or not directed from, or committed within, the country (paragraph 90.4(1)(b) and subsection 90.4(2)).

583. Because the definition of ***national security*** also covers foreign countries, the terms espionage, sabotage, terrorism, political violence and foreign interference are not further defined. This ensures that the terms are not limited by Australian concepts of these matters and are flexible to accommodate the meaning of these terms in foreign countries.

584. The definition also covers the protection of the integrity of a country's territory and borders from serious threats (paragraph 90.4(1)(c)). This is limited to 'serious' threats so that it does not include matters that, although rightly criminal, do not amount to national security threats, such as smuggling of illicit tobacco or other prohibited goods.

585. The definition also reflects the importance of international relationships to national security. Paragraphs 90.4(1)(d) and (e) deal with:

- the carrying out of the country's responsibilities to any other country in relation to:
    - the protection of the integrity of the country's territory and borders from serious threats, and
    - espionage, sabotage, terrorism, political violence and foreign interference (whether or not directed from, or committed within the country), and
- the country's political, military or economic relations with another country or other countries.

Section 90.5 – Definition of ***security classification***

586. Subsection 90.5(1) provides that ***security classification*** has the meaning prescribed by the regulations.

587. 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.

588. 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.

589. 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

590. 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.

591. Subsection 90.5(3) provides that, despite subsection 14(2) of the Legislation Act, regulations made for the purposes of subsection 90.5(1) may prescribe a matter by applying, adopting or incorporating any matter contained in an instrument or other writing as in force or existing from time to time.

592. This provision is included to allow the *Australian Government information security management guidelines – Australian Government security classification system* or other documents that exist as part of the Protective Security Policy Framework to be incorporated into the regulations if this is considered an efficient and appropriate manner of ensuring the definition of ***security classification*** is consistent with the Australian Government's policies relating to protective security. Importantly, these documents are all publicly available on the internet at www.protectivesecurity.gov.au.

Item 17

593. Item 17 repeals Division 91 of the Criminal Code, titled 'Offences relating to espionage and similar activities' and substitutes a new Division 91 titled 'Espionage'.

594. New Division 91 has three subdivisions:

- Subdivision A – Espionage
- Subdivision B – Espionage on behalf of foreign principal
- Subdivision C – Espionage-related offences.

595. Subdivision A introduces new tiered espionage offences to the Criminal Code.

- The most serious offence in section 91.1 applies where a person deals with information concerning Australia's national security and the person intended, or was reckless as to whether, their conduct would prejudice Australia's national security or advantage the national security of a foreign country. These offences are the most serious as the risks to Australia's national security are

far higher if a person is dealing with information that concerns Australia's national security.

- A second tier of offences in section 91.2 applies where a person deals with any information and the person intended, or was reckless as to whether, their conduct would prejudice Australia's national security. As these offences can be committed even if the information the person deals with does not relate to national security, the offences only apply where the person intends to prejudice Australia's national security.

- Section 91.3 applies where a person makes security classified information available to a foreign principal.

- A range of aggravating factors are set out at section 91.6, including where a person deals with high volumes of classified information or holds a security clearance.

596. The maximum penalties for the offences in Subdivision A range from life imprisonment to 20 years imprisonment. This reflects the extreme harm that is likely to result from the conduct covered by the offences and the threat that espionage poses to Australia's security, prosperity and sovereignty.

Division 91 - Espionage

Subdivision A - Espionage

Section 91.1 – Espionage – dealing with information etc. concerning national security which is or will be made available to a foreign principal

Intention as to national security

597. Subsection 91.1(1) will make it an offence for a person to deal with information or an article that is security classified or concerns Australia's national security where the person intends to prejudice Australia's national security or advantage the national security of a foreign country. The offence will only apply where the conduct has resulted in, or will result in the information or article being made available to a foreign principal.

598. This offence will carry a maximum penalty of life imprisonment.

599. An example of this offence is as follows. Person A is employed in a Commonwealth government department and has access to highly sensitive, classified information about Country Y's espionage activities in Australia and Australia's attempts to combat them. Person A has a close affiliation with Country Y, having spent time studying there during university and having become a specialist in the affairs of Country Y over the course of their employment with the Commonwealth. Person A makes a copy of one highly sensitive, classified document and takes it home. Person A hides the document in a spare room then makes contact with an official at Country Y's embassy to describe the content of the document and to offer to provide the document. Person Y intends to disclose the document because it would assist Country Y to avoid or disrupt Australia's activities. Person A arranges to leave the document in a particular location in suburban Canberra and a representative of Country Y collects it shortly thereafter.

600. To establish this offence, the prosecution will need to prove beyond reasonable doubt that:

- a person intentionally dealt with information or an article
- either:
    - the information or article had a security classification, or
    - the information or article concerns Australia's national security and the defendant is reckless as to this element
- the person intended that his or her conduct would prejudice Australia's national security or advantage the national security of a foreign country, and
- 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 and the person was reckless as to this.

601. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 91.1(1)(a) and (c). Intention is also the fault element for paragraph 91.1(1)(c). Under subsection 5.2(1) of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

602. Strict liability applies to the circumstance in subparagraph 91.1(1)(b)(i) consistent with subsection 91.1(3).

603. Recklessness is the fault element for subparagraph 91.1(1)(b)(ii) and paragraph 91.1(1)(d). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and
- a result if he or she is 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 the risk.

604. For paragraph 91.1(1)(a) the prosecution will have to prove beyond reasonable doubt that the defendant intentionally deals with information or an article. Consistent with the definition of ***deals*** in section 90.1, this may include receiving, obtaining, collecting, possessing, making a record or copying, altering, concealing, communicating, publishing or making available the information or article. In the example of the offence above, Person A has 'dealt' with the information by:

- copying the document
- concealing the document (by hiding it in the spare room)

- communicating the information (by describing the content of the document to the embassy official), and

- making the document available (by leaving it in the prearranged location in suburban Canberra)

605. For subparagraph 91.1(1)(b)(i), the prosecution will need to prove beyond a reasonable doubt that the information has a security classification. In accordance with subsection 91.1(3), strict liability will apply to this paragraph. Strict liability is set out in section 6.1 of the Criminal Code. The effect of applying strict liability to an element of an offence means that no fault element needs to be proved and the defence of mistake of fact is available.

606. Applying strict liability to this element of the offence is appropriate because information or articles carrying a security classification are clearly marked with the security classification and any person who has access to security classified information should easily be able to identify as such.

607. The defence of mistake of fact is set out in section 9.2 of the Criminal Code. The defence provides that a person is not criminally responsible for an offence that includes a physical element to which strict liability applies if:

- at or before the time of the conduct constituting the physical element, the person considered whether or not a fact existed, and is under a mistaken but reasonable belief about those facts, and

- had those facts existed, the conduct would not have constituted an offence.

608. The defendant bears an evidential burden in relation to this defence. Section 13.3 of the Criminal Code provides that in the case of a standard 'evidential burden' defence, the defendant bears the burden of pointing to evidence that suggests a reasonable possibility that the defence is made out. If this is done, the prosecution must refute the defence beyond reasonable doubt (section 13.1).

609. This defence would be available if, for example, a defendant had specifically turned his or her mind to whether the information or article had a security classification and had mistakenly, but reasonably, concluded that the information or article did not have a security classification.

610. ***Security classification*** is defined in section 90.5, to be inserted by Item 16 of Schedule 1. The definition will be prescribed in the regulations by reference to the protective security policies of the Commonwealth.

611. For subparagraph 91.1(1)(b)(ii), the prosecution will need to prove that the information or article dealt with by the defendant concerned Australia's national security. Consistent with the definition of ***national security*** in section 90.4, this could include information or articles relating to:

- the defence of Australia (paragraphs 90.4(1)(a) and (e) and 90.4(2)(e))

- Australia's border protection (paragraph 90.4(1)(c))

- activities of Australia's intelligence agencies, including ASIO (subsection 90.4(2)), and

- Australia's relationships with other countries (paragraph 90.4(1)(e)).

612. In the example above, the information in the document 'concerns national security' because it relates to Australia's intelligence activities to prevent Country Y from engaging in espionage in Australia and falls within paragraph 90.4(1)(b) of the definition of ***national security***.

613. The prosecution will also have to prove that the defendant was reckless as to whether the information or article concerns Australia's national security. Therefore, the defendant must have been aware of a substantial risk that the information concerns Australia's national security and, having regard to the circumstances known to him or her it was unjustifiable to take that risk.

614. For paragraph 91.1(1)(c), the prosecution will have to prove beyond reasonable doubt that the defendant intended that his or her conduct would prejudice Australia's national security or advantage the national security of a foreign country.

615. The term 'prejudice' is intended to capture a broad range of intended conduct, including an intention to harm or injure Australia's national security or to cause disadvantage to Australia. The term is also intended to cover impairment or loss to Australia's national security interests. 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.

616. The term 'advantage' is intended to capture an intention to put another country's national security in a favourable or superior position than it would have been without the communication of this information.

617. For subparagraph 91.1(1)(c)(ii), the person must intend to advantage the national security of a 'foreign country', not a 'foreign principal'. This is because the interests of countries in relation to 'national security' are unique and often relate to the protection to the territory of the country.

618. ***Foreign country*** is intended to cover countries other than Australia and is defined in the Dictionary to the Criminal Code as including:

- a colony or overseas territory

- a territory outside Australia, where a foreign country is to any extent responsible for the international relations of the territory, and

- a territory outside Australia that is, to some extent self-governing, but that is not recognised as an independent sovereign state by Australia.

619. In the example listed above, Person A has dealt with the document intending to advantage the national security of a foreign country. Person A made the document available to Country Y to allow them to successfully pursue espionage activities in Australia.

620. Whether or not the prejudice to Australia's national security or advantage to the national security of the foreign country occurs or the conduct is capable of bringing it about is not relevant to the defendant's culpability for the offence. For example, if the foreign country already had a copy of the document provided by the defendant then the disclosure by the defendant may not prejudice Australia's national security of advantage the national security of the foreign principal).

621. Consistent with subsection 91.1(4), for the purposes of subparagraph 91.1(1)(c)(ii) the person does not need to have in mind a particular foreign country and may have in mind more than one foreign country. For example, a person may be in possession of classified information and be willing to pass the information to whichever country is the highest bidder. The person may still be reckless as to whether passing the information to a foreign country will prejudice the national security of Australia or advantage the national security of a foreign country.

622. For paragraph 91.1(1)(d), the prosecution will have to prove beyond reasonable doubt that the defendant's conduct resulted in, or would result in, the information or article being made available to a foreign principal. The prosecution must also prove that the defendant was reckless as to this element. Therefore, the defendant must have been aware of a substantial risk that the information or article would be made available to a foreign principal and, having regard to the circumstances known to him or her, it is unjustifiable to take the risk.

623. In the example above, Person A was aware that Country Y would collect the document from the prearranged location and Country Y did collect it. By leaving the document in that location, Person A was aware of a substantial risk that the document would be made available to Country Y. Person A would also have been aware that it was unjustifiable to take the risk given the highly sensitive nature of the classified document.

624. Consistent with subsection 91.1(5), for the purposes of paragraph 91.1(1)(d), the person will not need to have in mind a particular foreign principal and may have in mind more than one foreign principal. For example, a defendant may assist an individual who has identified themselves to the defendant as a foreign official, but has not specified which foreign country they represent. Or, a defendant may provide assistance in the knowledge this assistance will or could assist multiple foreign principals at the same time.

625. The maximum penalty for this offence is life imprisonment. The maximum penalty needs to be adequate to deter and punish a worst case offence, including repeat offences. For the offence at subsection 91.1(1), the worst case scenario is a person disclosing highly classified information to a foreign country, intending to prejudice Australia's national security. The risks that may be posed to Australia's safety and security by such a disclosure are extreme and it is appropriate that the offence be punishable by the most serious penalty of life imprisonment.

626. The Note to subsection 91.1(1) specifies that an alternative verdict may be available for an offence against section 91.1(1) in accordance with section 93.5.

Reckless as to national security

627. Subsection 91.1(2) will make it an offence for a person to deal with information or a article that is security classified or concerns Australia's national security where the person is

reckless as to whether their conduct will prejudice Australia's national security or advantage the national security of a foreign country and where the conduct has resulted in, or will result in, the information or article being made available to a foreign principal.

628. This offence will carry a maximum penalty of 25 years imprisonment.

629. An example of this offence is as follows. Person A is employed in a Commonwealth government department and has access to highly sensitive, classified information. Person A has an association with Person B, who is an academic and a citizen of Country X. Person B has told Person A that he provides advice and commentary on Australia's foreign policy activities to Country X and has strong links to government in Country X. Person B asks Person A to collect privileged/classified intelligence information about a topical issue involving Australia and Country X and provide it to Person B in exchange for money. Person B says that this information will assist him/her in providing advice to Country X. Person A accepts this request, searches the department's internal electronic files and locates a classified document which contains intelligence information about the Australian Government's position on the topical issue. Person A prints a copy of this document and provides this to Person B.

630. To establish this offence, the prosecution will need to prove beyond reasonable doubt that:

- a person intentionally dealt with information or an article
- either:
    - the information or article had a security classification, or
    - the information or article concerns Australia's national security and the person was reckless as to this element
- the person was reckless as to whether his or her conduct would prejudice Australia's national security or advantage the national security of a foreign country, and
- 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 and the person was reckless as to this.

631. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 91.1(2)(a). Under subsection 5.2(1) of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

632. Strict liability applies to the circumstance in subparagraph 91.1(2)(b)(i).

633. Recklessness is the fault element for subparagraph 91.1(2)(b)(ii) and paragraphs 91.1(2)(c) and (d). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and

- a result if he or she is 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 the risk.

634. For paragraph 91.1(2)(a) the prosecution will have to prove beyond a reasonable doubt that the defendant intentionally deals with information or an article. Consistent with the definition of ***deals*** in section 90.1, this may include receiving, obtaining, collecting, possessing, making a record or copying, altering, concealing, communicating, publishing or making available the information or article. In the example of the offence above, Person A has 'dealt' with the information by:

- obtaining the information (by making an active effort to search the department's internal files for intelligence information on the topical issue)

- copying the document by printing it, and

- making it available (by passing the document to Person B).

635. For subparagraph 91.1(2)(b)(i), the prosecution will need to prove beyond a reasonable doubt that the information has a security classification. In accordance with subsection 91.1(3), strict liability will apply to this subparagraph. Strict liability is set out in section 6.1 of the Criminal Code. The effect of applying strict liability to an element of an offence means that no fault element needs to be proved and the defence of mistake of fact is available.

636. Applying strict liability to this element of the offence is appropriate because information or articles carrying a security classification are clearly marked with the security classification and any person who has access to security classified information should easily be able to identify as such.

637. The defence of mistake of fact is set out in section 9.2 of the Criminal Code. The defence provides that a person is not criminally responsible for an offence that includes a physical element to which strict liability applies if:

- at or before the time of the conduct constituting the physical element, the person considered whether or not a fact existed, and is under a mistaken but reasonable belief about those facts, and

- had those facts existed, the conduct would not have constituted an offence.

638. The defendant bears an evidential burden in relation to this defence. Section 13.3 of the Criminal Code provides that in the case of a standard 'evidential burden' defence, the defendant bears the burden of pointing to evidence that suggests a reasonable possibility that the defence is made out. If this is done, the prosecution must refute the defence beyond reasonable doubt (section 13.1).

639. This defence would be available if, for example, a defendant had specifically turned his or her mind to whether the information or article had a security classification and had mistakenly, but reasonably, concluded that the information or article did not have a security classification.

640. ***Security classification*** is defined in section 90.5, to be inserted by Item 16 of Schedule 1. The definition will be prescribed in the regulations by reference to the protective security policies of the Commonwealth.

641. For subparagraph 91.1(2)(b)(ii), the prosecution will need to prove that the information or article dealt with by the defendant concerned Australia's national security. Consistent with the definition of ***national security*** in section 90.4, this could include information or articles relating to:

- the defence of Australia (paragraphs 90.4(1)(a) and (e) and 90.4(2)(e))
- Australia's border protection (paragraph 90.4(1)(c))
- activities of Australia's intelligence agencies, including ASIO (subsection 90.4(2)), and
- Australia's relationships with other countries (paragraph 90.4(1)(e)).

642. In the example above, the information in the document 'concerns national security' because it is intelligence information on a topic issue involving Australia and another country and falls within paragraph 90.4(1)(e) of the definition of ***national security***. Depending on the topic, the information may also relate to other categories of national security in section 90.4. For example, the topical issue may relate to the Australia's military activities, in which case it could fall within paragraphs 90.4(1)(a) or (c) of the definition of national security.

643. The prosecution will also have to prove that the defendant was reckless as to whether the information or article concerns Australia's national security. Therefore, the defendant must have been aware of a substantial risk that the information concerns Australia's national security and, having regard to the circumstances known to him or her it was unjustifiable to take that risk.

644. For subparagraph 91.1(2)(c)(ii), the prosecution will have to prove beyond reasonable doubt that the defendant was reckless as to whether his or her conduct would prejudice Australia's national security or advantage the national security of a foreign country. Therefore, the defendant must have been aware of a substantial risk that the information or article could 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.

645. The term 'prejudice' is intended to capture a broad range of intended conduct, including an intention to harm or injure Australia's national security or to cause disadvantage to Australia. The term is also intended to cover impairment or loss to Australia's national security interests. 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.

646. The term 'advantage' is intended to cover putting another country's national security in a favourable or superior position than it would have been without the communication of this information.

647. For paragraph 91.1(2)(c), the person must be reckless as to whether his or her conduct would advantage the national security of a 'foreign country'. This is because the interests of countries in relation to 'national security' are unique and often relate to the protection to the territory of the country.

648. ***Foreign country*** is intended to cover countries other than Australia and is defined in the Dictionary to the Criminal Code as including:

- a colony or overseas territory
- a territory outside Australia, where a foreign country is to any extent responsible for the international relations of the territory, and
- a territory outside Australia that is, to some extent self-governing, but that is not recognised as an independent sovereign state by Australia.

649. In the example listed above, Person A has dealt with the document reckless as to whether it would prejudice Australia's national security or advantage the national security of a foreign country. Person A knows that Person B is a citizen of Country X and that Person B advises, and has strong links to government, in Country X. Therefore, Person A would be aware of the substantial risk that providing intelligence information about Australia's position on the topical issue to Person B would assist Country X to devise a strategy which effectively counters Australia's position in favour of Country X's interests.

650. Whether or not the prejudice to Australia's national security or advantage to the national security of a foreign country occurs or the conduct is capable of bringing it about is not relevant to the defendant's culpability for the offence. For example, if the foreign country already had a copy of the document provided by the defendant then the disclosure by the defendant may not prejudice Australia's national security of advantage the national security of the foreign actor).

651. Consistent with subsection 91.1(4), for the purposes of subparagraph 91.1(2)(c)(ii), the person does not need to have in mind a particular foreign country and may have in mind more than one foreign country. For example, a person may be in possession of classified information and be willing to pass the information to whichever country is the highest bidder. the person may still be reckless as to whether passing the information to a foreign country will prejudice the national security of Australia or advantage the national security of a foreign country.

652. For paragraph 91.1(2)(d), the prosecution will have to prove beyond reasonable doubt that the defendant's conduct resulted in, or would result in, the information or article being made available to a foreign principal. The prosecution must also prove that the person was reckless as to this element. Therefore, the defendant must have been aware of a substantial risk that the information or article would be made available to a foreign principal and, having regard to the circumstances known to him or her, it is unjustifiable to take the risk.

653. In the example above, Person A is aware that Person B provides advice to, and has strong links in, the government of Country X. Person B has told Person A that the information he/she provides will assist Person B in advising the government of Country X. By providing Person B with the document, Person A was aware of the substantial risk that the document or information in the document would be made available to Country Y. Person A would be aware that it was unjustifiable to take that risk given that the document contained sensitive/classified intelligence information.

654. Consistent with subsection 91.1(5), for the purposes of paragraph 91.1(2)(d), the person will not need to have in mind a particular foreign principal and may have in mind more than one foreign principal. For example, a defendant may assist an individual who has identified themselves to the defendant as a foreign official, but has not specified which foreign country they represent. Or, a defendant may provide assistance in the knowledge this assistance will or could assist multiple foreign principals at the same time.

655. The maximum penalty for this offence is 25 years imprisonment. The maximum penalty needs to be adequate to deter and punish a worst case offence, including repeat offences. For the offence at subsection 91.1(2), the worst case scenario is a person disclosing highly classified information to a foreign country, aware of a substantial risk that such a disclosure would prejudice Australia's national security. The risks that may be posed to Australia's safety and security by such a disclosure are extreme and it is appropriate that the offence be punishable by a serious penalty.

<u>Section 91.2 – Espionage – dealing with information etc. which is or will be made available to foreign principal</u>

Intention as to national security

656. Subsection 91.2(1) will make it an offence for a person to deal with information or a article where the person intends to prejudice Australia's national security or advantage the national security of a foreign country. The offence will only apply where the conduct has resulted in, or will result in the information or article being made available to a foreign principal.

657. This offence should carry a maximum penalty of 25 years imprisonment.

658. An example of this offence is as follows. Person A is a Commonwealth official employed as an analyst at a government department. Person A is strongly opposed to Australia's intention to negotiate a treaty with Country B. Person A compiles a report informed by the knowledge he has gained through his role as an analyst in the government department, which contains an aggregation of sensitive, but publically available, information – informed by expertise Person A has developed as a government analyst. Person A provides this to an official of Country B with the intention of convincing Country B not to negotiate the treaty with Australia, thereby harming Australia's international relations.

659. To establish this offence, the prosecution will need to prove beyond reasonable doubt that:

- a person intentionally dealt with information or an article

- the person intended that his or her conduct would prejudice Australia's national security, and

- 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 and the person was reckless as to this element.

660. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 91.2(1)(a). Intention also applies to paragraph 91.2(1)(b). Under subsection 5.2(1) of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

661. Recklessness is the fault element for paragraph 91.2(1)(c). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and

- a result if he or she is 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 the risk.

662. For paragraph 91.2(1)(a) the prosecution will have to prove beyond reasonable doubt that the defendant intentionally deals with information or an article. Consistent with the definition of ***deals*** in section 90.1, this may include receiving, obtaining, collecting, possessing, making a record or copying, altering, concealing, communicating, publishing or making available the information or article. In the example of the offence above, Person A has dealt with the information by collecting it, making a record of it in the report and communicating the report to Country B.

663. For paragraph 91.2(1)(b), the prosecution will have to prove beyond reasonable doubt that the defendant intended that his or her conduct would prejudice Australia's national security, as defined in section 90.4. Unlike the offences in section 91.1, a person will not commit the offence at subsection 91.2(1) if they hold an intention to advantage the national security of a foreign country. This is because the offences in section 91.2 apply to any information, not only information carrying a security classification or concerning Australia's national security.

664. The term 'prejudice' is intended to capture a broad range of intended conduct, including an intention to harm or injure Australia's national security or to cause disadvantage to Australia. The term is also intended to cover impairment or loss to Australia's national security interests. 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.

665. Whether or not the prejudice to Australia's national security or advantage to the national security of a foreign country occurs or the conduct is capable of bringing it about is not relevant to the defendant's culpability for the offence. For example, if the foreign country already knew the information provided by the defendant then the disclosure by the defendant may not prejudice Australia's national security.

666. For paragraph 91.2(1)(c), the prosecution will have to prove beyond reasonable doubt that the defendant's conduct resulted in, or would result in, the information or article being made available to a foreign principal. Recklessness is the fault element for this element. Therefore, the defendant must have been aware of a substantial risk that the information or article would be made available to a foreign principal and, having regard to the circumstances known to him or her, it is unjustifiable to take the risk.

667. In the example above, Person A has sent the report to Country B and would therefore have knowledge that the information was made available to a foreign principal.

668. Consistent with subsection 91.2(3), for the purpose of paragraph 91.2(1)(c), the person will not need to have in mind a particular foreign principal and may have in mind more than one foreign principal. For example, a defendant may assist an individual who has identified themselves to the defendant as a foreign official, but has not specified which foreign country they represent. Or, a defendant may provide assistance in the knowledge this assistance will or could assist multiple foreign principals at the same time.

669. The maximum penalty for this offence is 25 years imprisonment. The maximum penalty needs to be adequate to deter and punish a worst case offence, including repeat offences. For the offence at subsection 91.2(1), the worst case scenario is a person disclosing information to a foreign country, intending to prejudice Australia's national security. The risks that may be posed to Australia's safety and security by such a disclosure are extreme and it is appropriate that the offence be punishable by a serious penalty.

670. The Note to subsection 91.2(1) specifies that an alternative verdict may be available for an offence against section 91.2(1) in accordance with section 93.5.

Reckless as to national security

671. Subsection 91.2(2) will make it an offence for a person to deal with any information or a article where the person is reckless as to whether their conduct will prejudice Australia's national security and where the conduct has resulted in, or will result in, the information or article being made available to a foreign principal.

672. This offence will carry a maximum penalty of 20 years imprisonment.

673. An example of this offence is as follows. Person A is a Commonwealth official employed as an analyst at a government department. Person A is approached by Person B, a diplomat from Country X who is posted to Australia, and is offered a large sum of money if he can provide information which would assist Country X in undertaking intelligence operations in Australia. Person A compiles a report informed by the knowledge he has gained through his role as an analyst in the government department, which contains sensitive, but publically available, information about Australian interests. Person A sends the report to an email address provided by Person B at the embassy of Country X.

674. To establish this offence, the prosecution will need to prove beyond reasonable doubt that:

- a person intentionally dealt with information or an article

- the person was reckless as to whether his or her conduct would prejudice Australia's national security, and

- 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 and the person was reckless as to this element.

675. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 91.2(2)(a). Under subsection 5.2(1) of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

676. Recklessness is the fault element for paragraphs 91.2(2)(b) and (c). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and

- a result if he or she is 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 the risk.

677. For paragraph 91.2(2)(a) the prosecution will have to prove beyond a reasonable doubt that the defendant intentionally deals with information or an article. Consistent with the definition of ***deals*** in section 90.1, this may include receiving, obtaining, collecting, possessing, making a record or copying, altering, concealing, communicating, publishing or making available the information or article. In the example of the offence above, Person A has dealt with the information by collecting it, making a record of it in the report and communicating the report to Country X.

678. For paragraph 91.2(2)(b), the prosecution will have to prove beyond reasonable doubt that the defendant was reckless as to whether his or her conduct would prejudice Australia's national security. Unlike the offences in section 91.1, a person will not commit the offence at subsection 91.2(2) if they hold an intention to advantage the national security of a foreign country. This is because the offences in section 91.2 apply to any information, not only information carrying a security classification or concerning Australia's national security.

679. The defendant must have been aware of a substantial risk that the information or article could prejudice Australia's national security and, having regard to the circumstances known to him or her, it is unjustifiable to take the risk.

680. The term 'prejudice' is intended to capture a broad range of intended conduct, including an intention to harm or injure Australia's national security or to cause disadvantage to Australia. The term is also intended to cover impairment or loss to Australia's national security interests. 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.

681. Whether or not the prejudice to Australia's national security occurs or the conduct is capable of bringing it about is not relevant to the defendant's culpability for the offence. For

example, if the foreign country already knew the information provided by the defendant then the disclosure by the defendant may not prejudice Australia's national security.

682. For paragraph 91.2(2)(c), the prosecution will have to prove beyond reasonable doubt that the defendant's conduct resulted in, or would result in, the information or article being made available to a foreign principal. Recklessness is the fault element for this element. Therefore, the defendant must have been aware of a substantial risk that the information or article would be made available to a foreign principal and, having regard to the circumstances known to him or her, it is unjustifiable to take the risk.

683. Consistent with subsection 91.2(3), for the purposes of paragraph 91.2(2)(c), the person will not need to have in mind a particular foreign principal and may have in mind more than one foreign principal. For example, a defendant may assist an individual who has identified themselves to the defendant as a foreign official, but has not specified which foreign country they represent. Or, a defendant may provide assistance in the knowledge this assistance will or could assist multiple foreign principals at the same time.

684. The maximum penalty for this offence is 20 years imprisonment. The maximum penalty needs to be adequate to deter and punish a worst case offence, including repeat offences. For the offence at subsection 91.2(2), the worst case scenario is a person disclosing information to a foreign country, aware of a substantial risk that such a disclosure would prejudice Australia's national security. The risks that may be posed to Australia's safety and security by such a disclosure are very high and it is appropriate that the offence be punishable by a serious penalty.

Section 91.3 – Espionage – security classified information etc.

685. Section 91.3 will make it an offence for a person to deal with information or an article that has a security classification or concerns national security where the person is reckless as to whether their conduct has resulted in, or will result in, the information or article being made available to a foreign principal or a person acting on behalf of a foreign principal.

686. This offence will carry a maximum penalty of 20 years imprisonment.

687. Examples of this offence are as follows.

- Example 1: Person A is a Commonwealth official with access to classified information. Person A copies a document classified as TOP SECRET, makes contact with an official from Country X. Person A arranges to leave the document in an agreed public location and a representative of Country X collects it shortly thereafter.

- Example 2: Person B is a Commonwealth official. Person B meets Person C, who identifies themselves as an employee of a foreign 'think tank' that provides advice to the government of Country Y. Person B agrees to provide both open source and privileged information to Person C in exchange for money and other benefits. Person B is privy to classified conversations as part of his work. Person B details these conversations in the form of meeting notes meets Person C at a private location to relay the conversations and provide the notes. Person B does not apply a security classification to the notes but the content reveals capability gaps in the

Australian Intelligence Community's effort to combat espionage and foreign interference activities directed against Australia.

688. To establish this offence, the prosecution will need to prove beyond reasonable doubt that:

- a person intentionally dealt with information or an article
- the person's conduct results in, or will result in, the information or article being made available to a foreign principal or a person acting on behalf of a foreign principal and the person is reckless as to this element, and
- either:
    - the information or article has a security classification, or
    - the information or article concerns national security and the person is reckless as to this element.

689. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 91.3(1)(a). Under subsection 5.2(1) of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

690. Recklessness is the fault element for paragraph 91.3(1)(b) and subparagraph 91.3(1)(c)(ii). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and
- a result if he or she is 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 the risk.

691. Strict liability applies to the circumstance in subparagraph 91.3(1)(c)(i) consistent with subsection 91.3(3).

692. For paragraph 91.3(1)(a), the prosecution will have to prove beyond reasonable doubt that the defendant intentionally deals with information or an article. Consistent with the definition of ***deals*** in section 90.1, this may include receiving, obtaining, collecting, possessing, making a record or copying, altering, concealing, communicating, publishing or making available the information or article. In Example 1 above, Person A has dealt with the information by copying a document and making it available to Country X. In Example 2 above, Person B has dealt with the information by making a record of it in the form of meeting notes, communicating it, and making it available to Person C.

693. For paragraph 91.3(1)(b), the prosecution will have to prove beyond reasonable doubt that the defendant's conduct resulted in, or would result in, the information or article being made available to a foreign principal or person acting on behalf of a foreign principal. Recklessness is the fault element for this element. Therefore, the defendant must have been

aware of a substantial risk that the information or article would be made available to a foreign principal and, having regard to the circumstances known to him or her, it is unjustifiable to take the risk.

694. In Example 1 above, Person A is aware that Country X would collect the document from a prearranged location. By leaving that document in that location, Person A was aware of the substantial risk that the document would be made available to Country X. Similarly, in Example 2 above, Person B is aware that Person C works for an entity that provides advice to the government of Country Y. By providing Person C with the meeting notes, Person B is aware of the substantial risk that the document would be made available to Country Y. Both Person A and Person B would have been aware that it is unjustifiable to take that risk given the sensitive nature of the TOP SECRET document and the classified conversations, respectively.

695. Consistent with subsection 91.3(2), for the purposes of paragraph 91.3(1)(b), the person will not need to have in mind a particular foreign principal and may have in mind more than one foreign principal. For example, a defendant may assist an individual who has identified themselves to the defendant as a foreign official, but has not specified which foreign country they represent. Or, a defendant may provide assistance in the knowledge this assistance will or could assist multiple foreign principals at the same time.

696. For subparagraph 91.3(1)(c)(i), the prosecution will need to prove beyond a reasonable doubt that the information or article has a security classification. Consistent with subsection 91.3(3), strict liability will apply to this subparagraph. Strict liability is set out in section 6.1 of the Criminal Code. The effect of applying strict liability to an element of an offence means that no fault element needs to be proved and the defence of mistake of fact is available.

697. Applying strict liability to this element of the offence is appropriate because information or articles carrying a security classification are clearly marked with the security classification and any person who has access to security classified information should easily be able to identify as such.

698. The defence of mistake of fact is set out in section 9.2 of the Criminal Code. The defence provides that a person is not criminally responsible for an offence that includes a physical element to which strict liability applies if:

- at or before the time of the conduct constituting the physical element, the person considered whether or not a fact existed, and is under a mistaken but reasonable belief about those facts, and

- had those facts existed, the conduct would not have constituted an offence.

699. The defendant bears an evidential burden in relation to this defence. Section 13.3 of the Criminal Code provides that in the case of a standard ‘evidential burden’ defence, the defendant bears the burden of pointing to evidence that suggests a reasonable possibility that the defence is made out. If this is done, the prosecution must refute the defence beyond reasonable doubt (section 13.1).

700. This defence would be available if, for example, a defendant had specifically turned his or her mind to whether the information or article had a security classification and had

mistakenly but reasonably concluded that the information or article did not have a security classification.

701. ***Security classification*** is defined in section 90.5, to be inserted by Item 16 of Schedule 1. The definition will be prescribed in the regulations by reference to the protective security policies of the Commonwealth.

702. In the first example above, Person A has dealt with a document containing a security classification of 'TOP SECRET'. The prosecution would need to prove this physical element beyond a reasonable doubt, but would not need to prove any fault element.

703. For subparagraph 91.3(1)(c)(ii), the prosecution will need to prove that the information or article dealt with by the defendant concerned Australia's national security. Consistent with the definition of ***national security*** in section 90.4, this could include information or articles relating to:

- the defence of Australia (paragraphs 90.4(1)(a) and (e) and 90.4(1)(e))
- Australia's border protection (paragraph 90.4(1)(c))
- activities of Australia's intelligence agencies, including ASIO (subsection 90.4(2)), and
- Australia's relationships with other countries (paragraph 90.4(1)(e)).

704. In Example 2 above, the information contained in Person B's meeting notes 'relates to national security' because it reveals capability gaps in the Australian Intelligence Community's counter espionage and foreign interference effort and falls within paragraph 90.4(1)(b) of the definition of ***national security***.

705. The prosecution will also have to prove that the defendant was reckless as to whether the information or article concerns Australia's national security. Therefore, the defendant must have been aware of a substantial risk that the information concerns Australia's national security (as defined in section 90.4) and, having regard to the circumstances known to him or her it was unjustifiable to take that risk.

706. The maximum penalty for this offence is 20 years imprisonment. The maximum penalty needs to be adequate to deter and punish a worst case offence, including repeat offences. For the offence at subsection 91.3, the worst case scenario is a person disclosing highly classified information to a foreign country. The risks that may be posed to Australia's safety and security by such a disclosure are very high and it is appropriate that the offence be punishable by a serious penalty.

<u>Section 91.4 – Defences</u>

707. The general defences available under Part 2.3 of the Criminal Code will be available to a person accused of an offence under Subdivision A. In addition, section 91.4 creates specific defences.

708. The offences in Subdivision A are only intended to apply where a person's dealing with information is not a proper or legitimate part of their work. There are a vast range of

legitimate circumstances in which public officials deal with information concerning Australia's national security (including highly classified information) in performing their duties. For example, possessing or copying information concerning national security is a day to day occurrence in many Commonwealth departments and agencies and for Ministers and their staff. It is not intended to criminalise these dealings.

709. 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 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 evidentiary burden of proof on the defendant.

710. 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.

711. 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.

712. Consistent with section 13.3 of the Criminal Code, in the case of an evidential burden, the defendant bears the burden of adducing or pointing to evidence that suggests a reasonable possibility that the matter exists or does not exist. If the defendant discharges an evidential burden, the prosecution must disprove those matters beyond reasonable doubt, consistent with section 13.1 of the Criminal Code.

713. Subsection 91.4(1) will provide a defence if a person dealt with the relevant information or article:

- in accordance with a law of the Commonwealth (paragraph 91.4(1)(a)), or
- in accordance with an arrangement or agreement to which the Commonwealth is party and which allows for the exchange of information or articles (paragraph 91.4(1)(b)), or
- in the person's capacity as a public official (paragraph 91.4(1)(c)).

714. Section 10.5 of the Criminal Code provides a general defence of lawful authority applicable to all Commonwealth offences. This defence is narrow and only applies to conduct that is specifically justified or excused by a law. Consistent with the definition of ***law*** in the Dictionary to the Criminal Code, this means the conduct must be specifically justified or excused by a law of the Commonwealth, and includes the Criminal Code.

715. The defence at paragraph 91.4(1)(a) is broader than the lawful authority defence available under section 10.5 and will cover a person acting 'in accordance' with a law of the

Commonwealth, rather than the law of the Commonwealth needing to specifically justify or excuse the person's conduct.

716. The defence at paragraph 91.4(1)(b) applies when person dealt with the information or article in accordance with an agreement or arrangement to which the Commonwealth is party allowing for the exchange of information or articles. Many departments and agencies share information with international counterparts as part of their normal business dealings. Often this information is highly sensitive and highly classified. This defence provides that the espionage offences in Subdivision A do not apply if a person was sharing information or articles in accordance with an agreement or arrangement to which the Commonwealth was a party and which allows for the exchange of information or articles.

717. The terms 'arrangement' and 'agreement' are not defined and will be given their ordinary meaning. The term 'agreement' is not intended to be limited by the meaning of 'agreement' in Australian international practice as being a treaty, nor is it intended to require evidence of a formal contractual or legal agreement. It is intended that such terms will capture agreements or arrangements in a range of forms, including those made by exchange of letters or as a memorandum of understanding.

718. The defence at paragraph 91.4(1)(c) applies when a person dealt with the information or article in the person's capacity as a public official. ***Public official*** is defined in the Dictionary to the Criminal Code to include:

- a Commonwealth public official
- an officer or employee of the Commonwealth or of a State or Territory
- an individual who performs work for the Commonwealth, or for a State or Territory, under a contract
- an individual who holds or performs the duties of an office established by a law of the Commonwealth or of a State or Territory
- an individual who is otherwise in the service of the Commonwealth or of a State or Territory (including service as a member of a military force or police force)
- a member of the executive, judiciary or magistracy of the Commonwealth or of a State or Territory, and
- an officer or employee of:
    - an authority of the Commonwealth, or
    - an authority of a State or Territory.

719. ***Commonwealth public official*** is defined in the Dictionary to the Criminal Code to mean:

- the Governor-General

- a person appointed to administer the Government of the Commonwealth under section 4 of the Constitution
- a Parliamentary Secretary
- a member of either House of the Parliament
- an individual who holds an appointment under section 67 of the Constitution
- the Administrator, an Acting Administrator, or a Deputy Administrator, of the Northern Territory
- a Commonwealth judicial officer (as defined in the Dictionary to the Criminal Code)
- an APS employee
- an individual employed by the Commonwealth other than under the *Public Service Act 1999*
- a member of the Australian Defence Force
- a member or special member of the AFP
- an individual (other than an official of a registered industrial organisation) who holds or performs the duties of an office established by or under a law of the Commonwealth, other than:
    - the *Corporations (Aboriginal and Torres Strait Islander) Act 2006*
    - the *Australian Capital Territory (Self-Government) Act 1988*
    - the *Corporations Act 2001*
    - the *Norfolk Island Act 1979*, or
    - the *Northern Territory (Self-Government) Act 1978*
- an officer or employee of a Commonwealth authority
- an individual who is a contracted service provider for a Commonwealth contract
- an individual who is an officer or employee of a contracted service provider for a Commonwealth contract and who provides services for the purposes (whether direct or indirect) of the Commonwealth contract
- an individual (other than an official of a registered industrial organisation) who exercises powers, or performs functions, conferred on the person by or under a law of the Commonwealth, other than:
    - the *Corporations (Aboriginal and Torres Strait Islander) Act 2006*

- the *Australian Capital Territory (Self-Government) Act 1988*
- the *Corporations Act 2001*
- the *Norfolk Island Act 1979*
- the *Northern Territory (Self-Government) Act 1978*, or
- a provision specified in the regulations

- an individual who exercises powers, or performs functions, conferred on the person under a law in force in the Territory of Christmas Island or the Territory of Cocos (Keeling) Islands (whether the law is a law of the Commonwealth or a law of the Territory concerned), or

- the Registrar, or a Deputy Registrar, of Aboriginal and Torres Strait Islander Corporations.

720. This defence is intended to apply where a person discloses information concerning Australia's national security in the person's capacity as a public official. This may include, for example, an employee duty statement, a policy guidance document or employee practice manual, or previous examples of the same conduct which has been authorised by superiors. It will not be a defence to a charge of espionage where a person has gone beyond their ordinary duties.

721. Note 1 under the defence at subsection 91.4(1) clarifies that the defendant will bear an evidentiary burden in relation to this defence. Consistent with section 13.3 of the Criminal Code, the defendant will need to point to evidence that suggests a reasonable possibility that the defence is made out. If this is done, the prosecution must refute the defence beyond reasonable doubt (section 13.1).

722. Both AFP and CDPP consider the availability of any defences when considering whether to investigate and prosecute criminal offences. In relation to prosecution decisions, the Prosecution Policy of the Commonwealth specifically requires the CDPP to take into account any lines of defence which are plainly open to, or have been indicated by, the alleged offender in deciding whether there is a reasonable prospect of a conviction being secured. Subsection 93.1 (to be inserted by Item 18 of Schedule 1) requires the Attorney-General consider whether the defendant's conduct is authorised under the defences in section 91.4 before providing his or her consent to the institution of proceedings for the commitment of a person for trial for an offence to which the defence applies.

723. Section 91.4(2) will insert a defence based on existing section 91.2 of the Criminal Code where the information or article has already been communicated or made available to the public with the authority of the Commonwealth.

724. The defence under section 91.4(2) only applies where the relevant information or article is in the public domain with the authority of the Commonwealth. This defence is expressly limited to information or articles which are communicated or made publically available on an authorised basis. It will not be a defence to a charge of espionage against Subdivision A where the information is initially communicated or made available without the authority of the Commonwealth in the nature of a 'leak'. For example, a person who, without

authority, places information regarding the security or defence of the Commonwealth on an obscure internet website and subsequently communicates that information to a foreign organisation for the purpose of giving an advantage to another country's security or defence will not be able to rely on this defence.

725. Note 1 under the defence at subsection 91.4(2) clarifies that the defendant will bear an evidentiary burden in relation to this offence. This is appropriate because the defendant should be readily able to point to evidence that they acquired the relevant information or article indirectly from a publically available source. Consistent with section 13.3 of the Criminal Code, the defendant will need to point to evidence that suggests a reasonable possibility that the defence is made out. If this is done, the prosecution must refute the defence beyond reasonable doubt (section 13.1).

Section 91.5 – Matters affecting sentencing for offence against subsection 91.1(1)

726. Section 91.5 provides that in sentencing a person convicted of an offence against subsection 91.1(1) (punishable by a maximum of life imprisonment), the court must consider the following circumstances (set out in paragraph 91.6(1)(b)), if relevant:

- whether the person dealt with information or an article that has a security classification of secret or above (paragraph 91.6(1)(b)(i))
- whether the person dealt with information or an article from a foreign intelligence agency (paragraph 91.6(1)(b)(ii))
- whether the person dealt with five or more records or articles each of which has a security classification (paragraph 91.6(1)(b)(iii))
- whether the person altered a record or article to remove or conceal its security classification (paragraph 91.6(1)(b)(iv)), or
- whether, at the time the person dealt with the information or thing, the person held an Australian Government security clearance (paragraph 91.6(1)(b)(v)).

727. The circumstances listed in paragraph 91.6(1)(b) are considered to be so serious as to warrant a specific aggravated offence with a higher maximum penalty reflecting a higher level of culpability. However, the offence against subsection 91.1(1) carries a maximum penalty of life imprisonment. It is not possible to impose a higher maximum penalty than this even if aggravating circumstances are present.

728. Section 91.5 provides that, in determining the sentence to be passed in respect of a person for an offence against subsection 91.1(1) (punishable by life imprisonment, the court must take into account any circumstances set out in paragraph 91.6(1)(b) that exist in relation to the commission of the offence.

729. If any of these circumstances exist, the CDPP will be required to prove the existence of the relevant aggravating circumstance beyond a reasonable doubt at the sentencing stage.

730. Subsection 91.5(2) makes it clear that the court only need consider the circumstances in so far as they are known to the court and relevant. In practice, the CDPP will raise matters relevant to sentencing with the court.

731. Paragraph 91.5(3) provides, to avoid doubt, that consideration of the circumstances listed in paragraph 91.6(1)(b) are in addition to any other matters to which the court must take into account when sentencing. Paragraph 91.5(3) gives as an example the matters listed in section 16A(2) of the Crimes Act that a sentencing court must take into account, such as:

- the nature and circumstances of the offence
- other relevant offences
- the personal circumstances of the victim
- the degree to which the person has shown contrition
- any guilty plea
- cooperation with law enforcement agencies in the investigation of the offence, and
- the character, antecedents, age, means and physical or mental condition of the person.

Section 91.6 – Aggravated espionage offence

732. Section 91.6 will create an aggravated espionage offence. This offence will apply where a person commits an offence against section 91.1 (Espionage – dealing with information etc. concerning national security which could be made available to a foreign principal), section 91.2 (Espionage – dealing with information etc. which is or will be made available to foreign principal) or section 91.3 (Espionage – security classified information), and where:

- the person dealt with information or an article that has a security classification of SECRET or above (paragraph 91.6(1)(b)(i))
- that the person dealt with information or an article from a foreign intelligence agency (paragraph 91.6(1)(b)(ii))
- that that the person dealt with 5 or more records or articles each of which has a security classification (paragraph 91.6(1)(b)(iii))
- that the person altered a record or article to remove or conceal its security classification (paragraph 91.6(1)(b)(iv)), or
- that at the time the person dealt with the information or article, the person held an Australian Government security clearance (paragraph 91.6(1)(b)(v)).

733. The aggravated offence will be punishable by a maximum penalty of:

- life imprisonment if the maximum penalty for the underlying offence is 25 years imprisonment, or

- 25 years imprisonment if the maximum penalty for the underling offence is 20 years imprisonment.

734. An example of this offence is as follows. Person A is employed as an IT systems administrator at a Commonwealth government intelligence agency. In this role, Person A had access a large volume of highly classified information and throughout his employment Person A copied 1000 electronic files from the department's internal holdings to a personal hard drive. Over 100 of the documents copied have a security classification, including one document classified as TOP SECRET and one document from a Five-Eyes partner intelligence agency. Person A sells copies of all 1000 documents to Country X for a large sum of money.

735. To establish the aggravated offence the prosecution will first need to prove beyond reasonable doubt that a person commits an underlying offence against section 91.1 (Espionage – dealing with information etc. concerning national security which could be made available to a foreign principal), section 91.2 (Espionage – dealing with information etc. which is or will be made available to foreign principal) or section 91.3 (Espionage – security classified information).

736. The prosecution will be required to establish beyond reasonable doubt all of the elements constituting the relevant underlying offence, including any fault elements applicable to that offence. The physical and fault elements constituting an offence against section 91.1, section 91.2 and section 91.3 are described above.

737. Subsection 91.6(2) provides that there is no fault element for the physical element described in paragraph 91.6(1)(a) other than the fault elements for the underlying offence. The underlying offences themselves have specific physical and fault elements that must be proved by the prosecution. The prosecution will be required to establish beyond reasonable doubt all of the elements constituting the relevant underlying offence, including any fault elements applicable to that offence. Subsection 91.6(2) makes clear that for the purposes of the offence in section 91.6, the prosecution does not need to prove any fault elements in addition to those fault elements already applying to the underlying offences.

738. In addition to establishing the underlying offence, the prosecution will need to prove at least one of the following additional elements in relation to the commission of the underlying offence:

- the person dealt with information or an article that has a security classification of SECRET or above (paragraph 91.6(1)(b)(i))

- that the person dealt with information or an article from a foreign intelligence agency (paragraph 91.6(1)(b)(ii))

- that that the person dealt with five or more records or articles each of which has a security classification (paragraph 91.6(1)(b)(iii))

- that the person altered a record or article to remove or conceal its security classification (paragraph 91.6(1)(b)(iv)), or

- that at the time the person dealt with the information or article, the person held an Australian Government security clearance (paragraph 91.6(1)(b)(v)).

739. Recklessness is the fault element for subparagraphs 91.6(1)(b)(i), (ii), (iv) and (v). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and

- a result if he or she is 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 the risk.

740. Strict liability applies to the aggravating factor in subparagraph 91.6(1)(b)(iii) that the person dealt with five or more records or articles each of which has a security classification.

741. For subparagraph 91.6(1)(b)(i), the prosecution will need to prove beyond reasonable doubt that the defendant was reckless as to whether the information or article he or she dealt with in relation to the underlying offence has a security classification of secret or above. A security classification of secret or above is intended to refer to a classification in accordance with the Australian Government's Protective Security Policy Framework (PSPF) and represents an assessment that the disclosure of such information would likely cause serious or exceptionally grave damage to Australia's national interest, organisations or individuals.

742. In the example above, Person A copied and made available to Country X a document classified as TOP SECRET, which would fall within subparagraph 91.6(1)(b)(i).

743. The prosecution will have to prove that the defendant was reckless as to whether the information or thing has a security classification of secret or above. Therefore, the defendant must have been aware of a substantial risk that the information or thing has a security classification of secret or above and, having regard to the circumstances known to him or her, it was unjustifiable to take that risk.

744. For subparagraph 91.6(1)(b)(ii), the prosecution will need to prove beyond reasonable doubt that the defendant was reckless as to whether the information or article he or she dealt with in relation to the underlying offence was from a foreign intelligence agency. ***Foreign intelligence agency*** will be defined in the Dictionary to the Criminal Code (as amended by Item 24 of Schedule 1), as an intelligence or security service (however described) of a foreign country.

745. Information from foreign intelligence agencies is communicated to the Australian government in the highest confidence and with the expectation that all necessary steps will be taken to maintain the confidentially of such information. Espionage involving information from a foreign intelligence agency can therefore not only cause grave damage to Australia's national security and international relations, but also to the interests of foreign countries.

746. In the example above, Person A has dealt with information from a foreign intelligence agency because Person A copied a document from a Five-Eyes intelligence agency and made it available to Country X, which would fall within subparagraph 91.6(1)(b)(ii).

747. The prosecution will have to prove that the defendant was reckless as to whether the information or thing was from a foreign intelligence agency. Therefore, the defendant must have been aware of a substantial risk that the information or article is from a foreign

intelligence agency and, having regard to the circumstances known to him or her it was unjustifiable to take that risk.

748. For subparagraph 91.6(1)(b)(iii), the prosecution will need to prove beyond reasonable doubt that the defendant dealt with five or more records or articles, each of which has a security classification, in relation to the commission of the underlying offence. ***Security classification*** is defined in section 90.5, to be inserted by Item 16 of Schedule 1.

749. In accordance with subsection 91.6(3), strict liability applies to this subparagraph. Strict liability is set out in section 6.1 of the Criminal Code. The effect of applying strict liability to an element of an offence means that no fault element needs to be proved and the defence of mistake of fact is available.

750. Applying strict liability to subparagraph 91.6(1)(b)(iii) of the offence is appropriate because information or things carrying a security classification are clearly marked with the security classification and any person who has access to security classified information should easily be able to identify as such. It is not appropriate for a person to be able to avoid criminal responsibility for the aggravating factor at subparagraph 91.6(1)(b)(iii) by claiming, for example, that they knew they were dealing with three documents but not with five.

751. The defence of mistake of fact is set out in section 9.2 of the Criminal Code. The defence provides that a person is not criminally responsible for an offence that includes a physical element to which strict liability applies if:

- at or before the time of the conduct constituting the physical element, the person considered whether or not a fact existed, and is under a mistaken but reasonable belief about those facts, and

- had those facts existed, the conduct would not have constituted an offence.

752. The defendant bears an evidential burden in relation to this defence. Section 13.3 of the Criminal Code provides that in the case of a standard 'evidential burden' defence, the defendant bears the burden of pointing to evidence that suggests a reasonable possibility that the defence is made out. If this is done, the prosecution must refute the defence beyond reasonable doubt (section 13.1).

753. This defence would be available if, for example, a defendant had specifically turned his or her mind to whether he or she was dealing with records that had a security classification and had mistakenly but reasonably concluded that the records did not have a security classification.

754. For subparagraph 91.6(1)(b)(iv), the prosecution will need to prove beyond reasonable doubt that the defendant altered a record or article to remove or conceal its security classification.

755. ***Security classification*** is defined in section 90.5, to be inserted by Item 16 of Schedule 1. The definition will be prescribed in the regulations.

756. The terms 'altered', 'conceal' and 'remove' are not defined and are intended to take their ordinary meanings:

- The term *altered* is intended to cover the situation where a person amends or changes information in any way. This includes amending a classified document to change or delete the classification marker or to change specific terms in a document to remove identifying details while retaining the original meaning of the document.

- The term *conceals* is intended to cover hiding or preventing the security classification from being seen.

- The term *remove* is intended to cover erasing or taking away the security classification. This would include editing a document to delete the security classification.

757. Removing or altering a security classification is an aggravating factor because the government imposes a security classification to a document to specifically denote the sensitivity of the information to Australian Government – and the removal or alteration of a security classification is an overt contravention of this key principle of protective security. Removing or altering security classifications can also help an individual evade detection in the process of removing a document from a secure environment.

758. For subparagraph 91.6(1)(b)(v), the prosecution will need to prove beyond reasonable doubt that the defendant was reckless as to whether he or she held an Australian Government security clearance at the time they committed the underlying offence. The prosecution will need to establish that the defendant was aware of a substantial risk that he or she held an Australian Government security clearance and, having regard to the circumstances known to him or her it was unjustifiable to take that risk.

759. *Australian Government security clearance* is not defined but is intended to capture security clearances granted by the Australian Government Security Vetting Agency or another government agency conducting and issuing security clearances under the Protective Security Policy Framework. It would capture, for example, security clearances from Baseline to Top Secret Positive Vetting level.

760. Subparagraph 91.6(1)(b)(v) is an aggravating factor because people who hold a security clearance will be aware of appropriate information handling practices and the importance of protecting information as part of the an application and screening processes to obtain the security clearance.

761. The aggravated offence will be punishable by a maximum penalty of life imprisonment if the maximum penalty for the underlying offence is 25 years imprisonment, or, 25 years imprisonment if the maximum penalty for the underlying offence is 20 years imprisonment.

762. The higher maximum penalty reflects the higher level of culpability associated with proof of the circumstances set out in paragraph 91.6(1)(b) and the extreme risk posed to Australia's national security in such cases. The penalty for the aggravated offence is consistent with the established principal of Commonwealth criminal law policy as set out in the Guide to Framing Commonwealth Offences to impose a higher penalty where the consequences of the offence are particularly dangerous or damaging.

763. Subsection 91.6(4) provides that, for the avoidance of doubt, a person does not commit the underlying offence if the person has a defence to the underlying offence. This provision makes clear that a person does not commit the underlying offence, and cannot therefore be found liable under the aggravated offence, if a defence applies to the underlying offence.

764. In addition to the general defences in Part 2.3 of the Criminal Code, section 91.4 includes defences that provide that a person does not commit an offence against section 91.1, section 91.2 and section 91.3 if the person dealt with the information or thing:

- in accordance with a law of the Commonwealth
- in accordance with an arrangement or agreement, to which the Commonwealth is party, allowing for the exchange of information and things
- in the person's capacity as a public official, or
- the information or article has already been communicated or made available to the public with the authority of the Commonwealth.

765. Subsection 91.6(5) clarifies that a person may be convicted of an offence against section 91.6 even if the person has not been convicted of the underlying offence. This subsection makes it clear that to be convicted of the aggravated offence a person does not have to be convicted of the underlying offence; rather a person only needs to have committed the underlying offence.

766. The note to section 91.6 clarifies that an alternative verdict, in accordance with section 93.5, may be available for an offence against this subsection. The purpose of this is to ensure that offenders who have committed an offence against section 91.1, 91.2 or 91.3 do not escape conviction on these lesser charges where an aggravating factor in paragraph 91.6(1)(b) cannot be proven beyond reasonable doubt, but the underlying offence can. If a jury hearing a prosecution for an offence against section 91.6 is satisfied that all elements of the offence against either section 91.1, 91.2 or 91.3 are proven beyond reasonable doubt except the aggravating factor in paragraph 91.6(1)(b), it is appropriate that it will be able to find the defendant guilty instead of an offence against subsection 91.1, 91.2 or 91.3.

Section 91.7 – Geographical jurisdiction

767. This section will apply Section 15.4 (extended geographical jurisdiction—Category D) to each offence against Subdivision A.

768. Under section 15.4, the effect of Category D geographical jurisdiction is that each offences against Subdivision C applies:

- whether or not the conduct constituting the alleged offence occurs in Australia, and
- whether or not a result of the conduct constituting the alleged offence occurs in Australia.

769. Category D geographical jurisdiction is appropriate because intelligence agencies may undertake key facets of espionage activities against Australia in foreign countries to conceal these activities from hostile authorities. For example, an official from Country X may direct Person X to travel to Country Y to physically pass classified documents to the foreign official, without Person X having to travel directly to Country X.

Subdivision B – Espionage on behalf of a foreign principal

Section 91.8 – Espionage on behalf of a foreign principal

Intention as to national security

770. Subsection 91.8(1) will make it an offence for a person to deal with information or an article where the person intends to prejudice Australia's national security or advantage the national security of a foreign country. The offence will only apply where the person is reckless as to whether his or her conduct involves the commission, by the person or any other person, of an offence against Subdivision A (espionage). The person's conduct must also have been directed by, funded by, supervised by or engaged in on behalf of a foreign principal or a person acting on behalf of a foreign principal.

771. This offence will carry a maximum penalty of 25 years imprisonment.

772. An example of this offence is as follows. Person A is an official of Country D temporarily located in Australia, but does not have diplomatic immunity. Person A knows Person B, an employee of a Commonwealth government department, and is aware that Person B is unhappy at work as he believes he has been overlooked for promotion. Person B tells Person A that he has made copies of classified information and is willing to pass it to Person A. Person A is keen to gain access to the documents as they would give Country D a significant advantage in upcoming treaty negotiations. Person A obtains the documents from Person B.

773. To establish this offence, the prosecution will need to prove beyond reasonable doubt that:

- a person intentionally dealt with information or an article
- the person intended that his or her conduct would prejudice Australia's national security or advantage the national security of a foreign country
- the person is reckless as to whether the conduct involves the commission, by the person or any other person, of an offence against Subdivision A (espionage), and
- the:
    - person engaged in the conduct on behalf of a foreign principal
    - person engaged in the conduct on behalf of a person acting on behalf of a foreign principal
    - person engaged in the conduct in collaboration with a foreign principal

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

and the person is reckless as to this element.

774. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 91.8(1)(a). Intention will also apply to paragraph 91.8(1)(b). Under subsection 5.2(1) of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

775. Recklessness is the fault element for paragraphs 91.8(1)(c) and (d). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and
- a result if he or she is 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 the risk.

776. For paragraph 91.8(1)(a) the prosecution will have to prove beyond reasonable doubt that the defendant intentionally deals with information or an article. Consistent with the definition of ***deals*** in section 90.1, this may include receiving, obtaining, collecting, possessing, making a record or copying, altering, concealing, communicating, publishing or making available the information or article. In the example of the offence above, Person A has 'dealt' with the information by obtaining the information from Person B.

777. For paragraph 91.8(1)(b), the prosecution will have to prove beyond reasonable doubt that the defendant intended that his or her conduct would prejudice Australia's national security or advantage the national security of a foreign country.

778. The term 'prejudice' is intended to capture a broad range of intended conduct, including an intention to harm or injure Australia's national security or to cause disadvantage to Australia. The term is also intended to cover impairment or loss to Australia's national security interests. 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.

779. The term 'advantage' is intended to capture an intention to put another country's national security in a favourable or superior position compared to Australia's position or to benefit or profit another's country's national security compared to Australia's national security.

780. For subparagraph 91.8(1)(b)(ii), the person must intend to advantage the national security of a 'foreign country', not a 'foreign principal'. This is because the interests of

countries in relation to 'national security' are unique and often relate to the protection to the territory of the country.

781. ***Foreign country*** is intended to cover countries other than Australia and is defined in the Dictionary to the Criminal Code as including:

- a colony or overseas territory
- a territory outside Australia, where a foreign country is to any extent responsible for the international relations of the territory, and
- a territory outside Australia that is, to some extent self-governing, but that is not recognised as an independent sovereign state by Australia.

782. In the example listed above, Person A has dealt with the document intending to advantage the national security of a foreign country by giving Country D an advantage in upcoming treaty negotiations.

783. Consistent with subsection 91.8(4), for the purposes of subparagraph 91.8(1)(b)(ii), the person does not need to have in mind a particular foreign country and may have in mind more than one foreign country. For example, a person may be in possession of classified information and be willing to pass the information to whichever country is the highest bidder. The person may still be reckless as to whether passing the information to a foreign country will prejudice the national security of Australia or advantage the national security of a foreign country.

784. For paragraph 91.8(1)(c), the prosecution will have to prove beyond a reasonable doubt that the person's is reckless as to whether the conduct involves the commission, by the person or any other person, of an offence against Subdivision A (espionage). Therefore, the defendant must have been aware of a substantial risk that his or her conduct, or the conduct of any other person, involves the commission of an offence under Subdivision A (espionage).

785. Subdivision A creates the following offences:

- Espionage – dealing with information etc. concerning national security which is or will be made available to a foreign principal (section 91.1)
- Espionage – dealing with information etc. which is or will be made available to a foreign principal (section 91.2), and
- Espionage – security classified information etc. (section 91.3).

786. In proving the element at paragraph 91.11(1)(c), it will not be necessary for the prosecution to prove the physical or fault elements of the offence against Subdivision A, only that the defendant was reckless as to whether the conduct involved the commission, by the defendant or any other person, of an offence against Subdivision A.

787. In the example above, Person A would be aware of a substantial risk that Person B was committing an espionage offence by passing classified information obtained from his employment as a government employee to a foreign embassy.

788. For paragraph 91.8(1)(d), the prosecution will have to prove beyond a reasonable doubt that the defendant's conduct was engaged in on behalf of, or in collaboration with, a foreign principal, on behalf of a person acting on behalf of a foreign principal, directed, funded or supervised by a foreign principal or a person acting on behalf of a foreign principal. Recklessness is the fault element for this element. Therefore, the defendant must have been aware of a substantial risk that his or her conduct was engaged in on behalf of, or in collaboration with, a foreign principal, on behalf of a person acting on behalf of a foreign principal, directed, funded or supervised by a foreign principal or a person acting on behalf of a foreign principal and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk.

789. It is possible that a defendant will know, or be reckless, as to the fact that they are engaging in conduct a foreign government because they are being tasked by a person who identifies himself or herself as an official of a foreign government. In this case, the person will be engaging in the conduct on behalf of the foreign principal.

790. However, it may also be the case that the defendant is not tasked directly by a foreign government official, but by an intermediary. In this case, the prosecution will have to prove beyond a reasonable doubt that the defendant was aware of a substantial risk that he or she was being tasked by a person acting on behalf of a foreign principal and that it was unjustifiable to take that risk. This may be the case where, for example, the intermediary advises the defendant that the intermediary acts in coordination with foreign officials, or the intermediary facilitates preferential treatment for the defendant from a foreign government.

791. Consistent with subsection 91.8(5), for the purposes of paragraph 91.8(1)(d), the person will not need to have in mind a particular foreign principal and may have in mind more than one foreign principal. For example, a defendant may assist an individual who has identified themselves to the defendant as a foreign official, but has not specified which foreign country they represent. Or, a defendant may provide assistance in the knowledge this assistance will or could assist multiple foreign principals at the same time.

792. The maximum penalty for this offence is 25 years imprisonment. The maximum penalty needs to be adequate to deter and punish a worst case offence, including repeat offences. This offence punishes the foreign actor who engages in espionage against the Australian government. For the offence at subsection 91.8(1), the worst case scenario is a foreign person receiving highly classified information, aware of a substantial risk that the information has been provided due to the commission of an espionage offence, with an intention to prejudice Australia's national security. The risks that may be posed to Australia's safety and security by such a disclosure are very high and it is appropriate that the offence be punishable by a serious penalty.

793. The Note to subsection 91.8(1) specifies that an alternative verdict may be available for an offence against section 91.8(1) in accordance with section 93.5.

Reckless as to national security

794. Subsection 91.8(2) will make it an offence for a person to deal with information or a article where the person is reckless as to whether the person's conduct will prejudice Australia's national security or advantage the national security of a foreign country. The offence will only apply where the person is reckless as to whether his or her conduct involves the commission, by the person or any other person, of an offence against Subdivision A

(espionage). The person's conduct must also have been directed by, funded by, supervised by or engaged in on behalf of a foreign principal or a person acting on behalf of a foreign principal.

795. This offence will carry a maximum penalty of 20 years imprisonment.

796. An example of this offence is as follows. Person A is an Australian citizen with close links to the intelligence services of Country D. Person A acts as an intermediary for Country D in Australia and receives information from a former employee of a defence contractor who engages in work for the Commonwealth. Person A believes that access to the information could assist Country D to gain an advantage over Australia's armed forces. Person A passes the information to the intelligence service of Country D.

797. To establish this offence, the prosecution will need to prove beyond reasonable doubt that:

- a person intentionally dealt with information or an article
- the person is reckless as to whether his or her conduct would prejudice Australia's national security or advantage the national security of a foreign country
- the person is reckless as to whether the conduct involves the commission, by the person or any other person, of an offence against Subdivision A (espionage), and
- the:
    - person engaged in the conduct on behalf of a foreign principal
    - person engaged in the conduct on behalf of a person acting on behalf of a foreign principal
    - person engaged in the conduct in collaboration with a foreign principal
    - person engaged in the conduct in collaboration with a person acting on behalf of a foreign principal
    - conduct was directed, funded or supervised by a foreign principal, or
    - conduct was directed, funded or supervised by a person acting on behalf of a foreign principal

  and the person is reckless as to this element.

798. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 91.8(2)(a). Under subsection 5.2(1) of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

799. Recklessness is the fault element for paragraphs 91.8(2)(b), (c) and (d). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and

- a result if he or she is 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 the risk.

800. For paragraph 91.8(2)(a) the prosecution will have to prove beyond reasonable doubt that the defendant intentionally deals with information or n article. Consistent with the definition of ***deals*** in section 90.1, this may include receiving, obtaining, collecting, possessing, making a record or copying, altering, concealing, communicating, publishing or making available the information or an article. In the example of the offence above, Person A has 'dealt' with the information by receiving the information from the former employee of a defence contractor and communicating the information to the intelligence service of Country D.

801. For paragraph 91.8(2)(b), the prosecution will have to prove beyond reasonable doubt that the defendant is reckless as to whether his or her conduct would prejudice Australia's national security or advantage the national security of a foreign country. Therefore, the defendant will need to be aware of a substantial risk that his or her conduct will 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 that risk.

802. The term 'prejudice' is intended to capture a broad range of intended conduct, including an intention to harm or injure Australia's national security or to cause disadvantage to Australia. The term is also intended to cover impairment or loss to Australia's national security interests. 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.

803. The term 'advantage' is intended to capture an intention to put another country's national security in a favourable or superior position compared to Australia's position or to benefit or profit another's country's national security compared to Australia's national security.

804. For subparagraph 91.8(2)(b)(ii), the person must intend to advantage the national security of a 'foreign country', not a 'foreign principal'. This is because the interests of countries in relation to 'national security' are unique and often relate to the protection to the territory of the country.

805. ***Foreign country*** is intended to cover countries other than Australia and is defined in the Dictionary to the Criminal Code as including:

- a colony or overseas territory

- a territory outside Australia, where a foreign country is to any extent responsible for the international relations of the territory, and

- a territory outside Australia that is, to some extent self-governing, but that is not recognised as an independent sovereign state by Australia.

806. In the example listed above, Person A is aware of a substantial risk that proving the information to Country D will advantage that country's national security by giving them an advantage over Australia's defence forces. Person A would be aware that in these circumstances, passing the information to a foreign country is unjustifiable.

807. Whether or not the prejudice to Australia's national security or advantage to the national security of a foreign country occurs or the conduct is capable of bringing it about is not relevant to the defendant's culpability for the offence. For example, if the foreign country already had a copy of the document provided by the defendant then the disclosure by the defendant may not prejudice Australia's national security.

808. Consistent with subsection 91.8(4), for the purposes of subparagraph 91.8(2)(b)(ii), the person does not need to have in mind a particular foreign country and may have in mind more than one foreign country. For example, a person may be in possession of classified information and be willing to pass the information to whichever country is the highest bidder. The person may still be reckless as to whether passing the information to a foreign country will prejudice the national security of Australia or advantage the national security of a foreign country.

809. For paragraph 91.8(2)(c), the prosecution will have to prove beyond a reasonable doubt that the person is reckless as to whether the conduct involves the commission, by the person or any other person, of an offence against Subdivision A (espionage). Therefore, the defendant must have been aware of a substantial risk that his or her conduct, or the conduct of any other person, involves the commission of an offence under Subdivision A (espionage).

810. Subdivision A creates the following offences:

- Espionage – dealing with information etc. concerning national security which could be made available to a foreign principal (section 91.1)
- Espionage – dealing with information etc. which is or will be made available to a foreign principal (section 91.2), and
- Espionage – security classified information etc. (section 91.3).

811. In proving the element at paragraph 91.8(2)(c), it will not be necessary for the prosecution to prove the physical or fault elements of the offence against Subdivision A, only that the defendant was reckless as to whether the conduct involved the commission, by the defendant or any other person, of an offence against Subdivision A.

812. In the example above, Person A would be aware of a substantial risk that they may be committing an espionage offence by passing sensitive information about defence matters to the intelligence service of a foreign government.

813. For paragraph 91.8(2)(d), the prosecution will have to prove beyond a reasonable doubt that the defendant's conduct was engaged in on behalf of, or in collaboration with, a foreign principal, on behalf of a person acting on behalf of a foreign principal, directed, funded or supervised by a foreign principal or a person acting on behalf of a foreign principal. Recklessness is the fault element for this element. Therefore, the defendant must have been aware of a substantial risk that his or her conduct was engaged in on behalf of, or in collaboration with, a foreign principal, on behalf of a person acting on behalf of a foreign

principal, directed, funded or supervised by a foreign principal or a person acting on behalf of a foreign principal and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk.

814. It is possible that a defendant will know, or be reckless, as to the fact that they are engaging in conduct a foreign government because they are being tasked by a person who identifies himself or herself as an official of a foreign government. In this case, the person will be engaging in the conduct on behalf of the foreign principal.

815. However, it may also be the case that the defendant is not tasked directly by a foreign government official, but by an intermediary. In this case, the prosecution will have to prove beyond a reasonable doubt that the defendant was aware of a substantial risk that he or she was being tasked by a person acting on behalf of a foreign principal and that it was unjustifiable to take that risk. This may be the case where, for example, the intermediary advises the defendant that the intermediary acts in coordination with foreign officials, or the intermediary facilitates preferential treatment for the defendant from a foreign government. .

816. Consistent with subsection 91.8(5), for the purposes of paragraph 91.8(2)(d) the person will not need to have in mind a particular foreign principal and may have in mind more than one foreign principal. For example, a defendant may assist an individual who has identified themselves to the defendant as a foreign official, but has not specified which foreign country they represent. Or, a defendant may provide assistance in the knowledge this assistance will or could assist multiple foreign principals at the same time.

817. The maximum penalty for this offence is 20 years imprisonment. The maximum penalty needs to be adequate to deter and punish a worst case offence, including repeat offences. This offence punishes the foreign actor who engages in espionage against the Australian government. For the offence at subsection 91.8(2), the worst case scenario is a foreign person receiving highly classified information due to the commission of an espionage offence, reckless as to whether Australia's national security will be prejudiced. The risks that may be posed to Australia's safety and security by such a disclosure are very high and it is appropriate that the offence be punishable by a serious penalty.

Conduct on behalf of a foreign principal

818. Subsection 91.8(3) will make it an offence for a person to deal with information or an article where the person is reckless as to whether his or her conduct involves the commission, by the person or any other person, of an offence against Subdivision A (espionage). The person's conduct must also have been directed by, funded by, supervised by or engaged in on behalf of a foreign principal or a person acting on behalf of a foreign principal.

819. This offence will carry a maximum penalty of 15 years imprisonment.

820. An example of this offence is as follows. Person A is an undeclared intelligence agent for Country B and is located in Australia. Person A has been cultivating Person C, an employee of a Commonwealth department, as a source. Person C knows that Person A works at Country B's embassy but is not aware that Person A is an intelligence officer. Person C provides Person A with a sensitive document about Country B from one of Australia's foreign partners. Person A passes that document on to their employer in Country B.

821. To establish this offence, the prosecution will need to prove beyond reasonable doubt that:

- a person intentionally dealt with information or an article
- the person is reckless as to whether the conduct involves the commission, by the person or any other person, of an offence against Subdivision A (espionage), and
- the:
    - person engaged in the conduct on behalf of a foreign principal
    - person engaged in the conduct on behalf of a person acting on behalf of a foreign principal
    - person engaged in the conduct in collaboration with a foreign principal
    - person engaged in the conduct in collaboration with a person acting on behalf of a foreign principal
    - conduct was directed, funded or supervised by a foreign principal, or
    - conduct was directed, funded or supervised by a person acting on behalf of a foreign principal

  and the person is reckless as to this element.

822. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 91.8(3)(a). Under subsection 5.2(1) of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

823. Recklessness is the fault element for paragraphs 91.8(3)(b) and (c). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and
- a result if he or she is 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 the risk.

824. For paragraph 91.8(3)(a) the prosecution will have to prove beyond reasonable doubt that the defendant intentionally deals with information or an article. Consistent with the definition of ***deals*** in section 90.1, this may include receiving, obtaining, collecting, possessing, making a record or copying, altering, concealing, communicating, publishing or making available the information or article. In the example of the offence above, Person A has 'dealt' with the information by obtaining the information from Person B.

825. For paragraph 91.8(3)(b), the prosecution will have to prove beyond a reasonable doubt that the person is reckless as to whether the conduct involves the commission, by the person or any other person, of an offence against Subdivision A (espionage). Therefore, the defendant must have been aware of a substantial risk that his or her conduct, or the conduct of any other person, involves the commission of an offence under Subdivision A (espionage).

826. Subdivision A creates the following offences:

- Espionage – dealing with information etc. concerning national security which could be made available to a foreign principal (section 91.1)
- Espionage – dealing with information etc. which is or will be made available to a foreign principal (section 91.2), and
- Espionage – security classified information etc. (section 91.3).

827. In proving the element at paragraph 91.8(3)(b), it will not be necessary for the prosecution to prove the physical or fault elements of the offence against Subdivision A, only that the defendant was reckless as to whether the conduct involved the commission, by the defendant or any other person, of an offence against Subdivision A.

828. In the example above, Person A would be aware of a substantial risk that they may be committing an espionage offence by passing a sensitive document from one of Australia's foreign partners to a foreign embassy.

829. For paragraph 91.8(3)(c), the prosecution will have to prove beyond a reasonable doubt that the defendant's conduct was engaged in on behalf of, or in collaboration with, a foreign principal, on behalf of a person acting on behalf of a foreign principal, directed, funded or supervised by a foreign principal or a person acting on behalf of a foreign principal. Recklessness is the fault element for this element. Therefore, the defendant must have been aware of a substantial risk that his or her conduct was engaged in on behalf of, or in collaboration with, a foreign principal, on behalf of a person acting on behalf of a foreign principal, directed, funded or supervised by a foreign principal or a person acting on behalf of a foreign principal and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk.

830. It is possible that a defendant will know, or be reckless, as to the fact that they are engaging in conduct a foreign government because they are being tasked by a person who identifies himself or herself as an official of a foreign government. In this case, the person will be engaging in the conduct on behalf of the foreign principal.

831. However, it may also be the case that the defendant is not tasked directly by a foreign government official, but by an intermediary. In this case, the prosecution will have to prove beyond a reasonable doubt that the defendant was aware of a substantial risk that he or she was being tasked by a person acting on behalf of a foreign principal and that it was unjustifiable to take that risk. This may be the case where, for example, the intermediary advises the defendant that the intermediary acts in coordination with foreign officials, or the intermediary facilitates preferential treatment for the defendant from a foreign government.

832. Consistent with subsection 91.8(5), for the purposes of paragraph 91.8(3)(c) the person will not need to have in mind a particular foreign principal and may have in mind

more than one foreign principal. For example, a defendant may assist an individual who has identified themselves to the defendant as a foreign official, but has not specified which foreign country they represent. Or, a defendant may provide assistance in the knowledge this assistance will or could assist multiple foreign principals at the same time.

833. The maximum penalty for this offence is 15 years imprisonment. The maximum penalty needs to be adequate to deter and punish a worst case offence, including repeat offences. This offence punishes the foreign actor who engages in espionage against the Australian government. For the offence at subsection 91.8(3), the worst case scenario is a foreign country receiving highly classified information due to the commission of an espionage offence. The risks that may be posed to Australia's safety and security by such a disclosure are very high and it is appropriate that the offence be punishable by a serious penalty.

Section 91.9 - Defences

834. The general defences available under Part 2.3 of the Criminal Code will be available to a person accused of an offence under Subdivision B. In addition, section 91.9 creates the following specific defences:

- the person dealt with the information or article in accordance with a law of the Commonwealth
- the person dealt with the information or article in accordance with an arrangement or agreement to which the Commonwealth is party and which allows for the exchange of information or articles, or
- the person dealt with the information or article in the person's capacity as a public official.

835. The offences in Subdivision B are only intended to apply where a person's dealing with information is not a proper or legitimate part of their work. There are a vast range of legitimate circumstances in which public officials deal with information concerning Australia's national security (including highly classified information) in performing their duties. For example, possessing or copying information concerning national security is a day to day occurrence in many Commonwealth departments and agencies and for Ministers and their staff. It is not intended to criminalise these dealings.

836. Paragraph 91.9(1)(a) creates a defence to a prosecution for an offence against Subdivision B that the person dealt with the information or article in accordance with the law of the Commonwealth.

837. 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 another country's security or defence (for example, subsection 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, section 91.9(1) casts the matter of lawful authority as a defence, which has the effect of placing an evidentiary burden of proof on the defendant.

838. If lawful authority was an element of the espionage offences in Subdivision B, 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 thing in the relevant manner. This is a significant barrier to prosecutions, especially in relation to the offences in Subdivision B, which target people acting on behalf of foreign principals who may have authority for their actions under foreign laws.

839. 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.

840. Consistent with section 13.3 of the Criminal Code, in the case of an evidential burden, the defendant bears the burden of adducing or pointing to evidence that suggests a reasonable possibility that the matter exists or does not exist. If the defendant discharges an evidential burden, the prosecution must disprove those matters beyond reasonable doubt, consistent with section 13.1 of the Criminal Code.

841. Section 10.5 of the Criminal Code provides a general defence of lawful authority applicable to all Commonwealth offences. This defence is narrow and only applies to conduct that is specifically justified or excused by a law. Consistent with the definition of ***law*** in the Dictionary to the Criminal Code, this means the conduct must be specifically justified or excused by a law of the Commonwealth.

842. The defence at paragraph 91.9(1)(a) is broader than the lawful authority defence available under section 10.5 and will cover a person acting 'in accordance' with a law of the Commonwealth, rather than the law of the Commonwealth needing to specifically justify or excuse the person's conduct.

843. Paragraph 91.9(1)(b) creates a defence to a prosecution for an offence against Subdivision B that the person dealt with the information or article in accordance with an agreement or arrangement to which the Commonwealth is party which allows for the exchange of information or things. Many departments and agencies share information with international counterparts as part of their normal business dealings. Often this information is highly sensitive and highly classified. This defence provides that the espionage offences in Subdivision B do not apply if a person was sharing information or things in accordance with an agreement or arrangement to which the Commonwealth was a party and which allows for the exchange of information or articles.

844. The terms 'arrangement' and 'agreement' are not defined and will be given their ordinary meaning. The term 'agreement' is not intended to be limited by the meaning of 'agreement' in Australian international practice as being a treaty, nor is it intended to require evidence of a formal contractual or legal agreement. It is intended that such terms will capture agreements or arrangements in a range of forms, including those made by exchange of letters or as a memorandum of understanding.

845. The defence at paragraph 91.9(1)(c) applies when a person dealt with the information or thing in the person's capacity as a public official. ***Public official*** is defined in the Dictionary to the Criminal Code to include:

- a Commonwealth public official
- an officer or employee of the Commonwealth or of a State or Territory
- an individual who performs work for the Commonwealth, or for a State or Territory, under a contract
- an individual who holds or performs the duties of an office established by a law of the Commonwealth or of a State or Territory
- an individual who is otherwise in the service of the Commonwealth or of a State or Territory (including service as a member of a military force or police force)
- a member of the executive, judiciary or magistracy of the Commonwealth or of a State or Territory, and
- an officer or employee of:
- an authority of the Commonwealth, or
- an authority of a State or Territory.

846. Commonwealth ***public official*** is defined in the Dictionary to the Criminal Code to mean:

- the Governor-General
- a person appointed to administer the Government of the Commonwealth under section 4 of the Constitution
- a Parliamentary Secretary
- a member of either House of the Parliament
- an individual who holds an appointment under section 67 of the Constitution
- the Administrator, an Acting Administrator, or a Deputy Administrator, of the Northern Territory
- a Commonwealth judicial officer (as defined in the Dictionary to the Criminal Code)
- an APS employee
- an individual employed by the Commonwealth other than under the Public Service Act 1999
- a member of the Australian Defence Force
- a member or special member of the AFP

- an individual (other than an official of a registered industrial organisation) who holds or performs the duties of an office established by or under a law of the Commonwealth, other than:
    - the Corporations (Aboriginal and Torres Strait Islander) Act 2006
    - the Australian Capital Territory (Self-Government) Act 1988
    - the Corporations Act 2001
    - the Norfolk Island Act 1979, or
    - the Northern *Territory (Self-Government) Act 1978*
- an officer or employee of a Commonwealth authority
- an individual who is a contracted service provider for a Commonwealth contract
- an individual who is an officer or employee of a contracted service provider for a Commonwealth contract and who provides services for the purposes (whether direct or indirect) of the Commonwealth contract
- an individual (other than an official of a registered industrial organisation) who exercises powers, or performs functions, conferred on the person by or under a law of the Commonwealth, other than:
    - the Corporations (Aboriginal and Torres Strait Islander) Act 2006
    - the Australian Capital Territory (Self-Government) Act 1988
    - the Corporations Act 2001
    - the Norfolk Island Act 1979
    - the Northern *Territory (Self-Government) Act 1978*, or
- a provision specified in the regulations
- an individual who exercises powers, or performs functions, conferred on the person under a law in force in the Territory of Christmas Island or the Territory of Cocos (Keeling) Islands (whether the law is a law of the Commonwealth or a law of the Territory concerned), or
- the Registrar, or a Deputy Registrar, of Aboriginal and Torres Strait Islander Corporations.

847. This defence is intended to apply where a person discloses information in the person's capacity as a public official. This may include, for example, an employee duty statement, a policy guidance document or employee practice manual, or previous examples of the same conduct which has been authorised by superiors. It will not be a defence to a charge of espionage where a person has gone beyond their ordinary duties.

848. Note 1 under the defence at subsection 91.9(1) clarifies that the defendant will bear an evidentiary burden in relation to this defence. Consistent with section 13.3 of the Criminal Code, the defendant will need to point to evidence that suggests a reasonable possibility that the defence is made out. If this is done, the prosecution must refute the defence beyond reasonable doubt (section 13.1).

849. Both AFP and CDPP consider the availability of any defences when considering whether to investigate and prosecute criminal offences. In relation to prosecution decisions, the Prosecution Policy of the Commonwealth specifically requires the CDPP to take into account any lines of defence which are plainly open to, or have been indicated by, the alleged offender in deciding whether there is a reasonable prospect of a conviction being secured. Subsection 93.1 (to be inserted by Item 18 of Schedule 1) requires the Attorney-General consider whether the defendant's conduct is authorised under the defences in section 91.14 before providing his or her consent to the institution of proceedings for the commitment of a person for trial for an offence to which the defence applies.

850. Section 91.9(2) will insert a defence based on existing section 91.2 of the Criminal Code where the information or thing has already been communicated or made available to the public with the authority of the Commonwealth.

851. The defence under section 91.9(2) only applies where the relevant information or thing is in the public domain with the authority of the Commonwealth. This defence is expressly limited to information or things which are communicated or made publically available on an authorised basis. It will not be a defence to a charge of espionage against Subdivision B where the information is initially communicated or made available without the authority of the Commonwealth in the nature of a 'leak'. For example, a person who, without authority, places information regarding the security or defence of the Commonwealth on an obscure internet website and subsequently communicates that information to a foreign organisation for the purpose of giving an advantage to another country's security or defence will not be able to rely on this defence.

852. Note 1 under the defence at subsection 91.9(2) clarifies that the defendant will bear an evidentiary burden in relation to this offence. This is appropriate because the defendant should be readily able to point to evidence that they acquired the relevant information or thing indirectly from a publically available source. Consistent with section 13.3 of the Criminal Code, the defendant will need to point to evidence that suggests a reasonable possibility that the defence is made out. If this is done, the prosecution must refute the defence beyond reasonable doubt (section 13.1).

Section 91.10 – Geographical jurisdiction

853. This section will apply Section 15.4 (extended geographical jurisdiction—Category D) to each offence against Subdivision B.

854. Under section 15.4, the effect of Category D geographical jurisdiction is that each offences against Subdivision C applies:

- whether or not the conduct constituting the alleged offence occurs in Australia, and

- whether or not a result of the conduct constituting the alleged offence occurs in Australia.

855. Category D geographical jurisdiction is appropriate because intelligence agencies may undertake key facets of espionage activities against Australia in foreign countries to conceal these activities from relevant authorities seeking to prevent these activities. For example, an official from Country X may establish contact with Australian Person Y while on official travel in Country Z, and obtain Person Y's agreement to conduct espionage on their return to Australia.

Subdivision C – Espionage-related offences

Section 91.11 – Offence of soliciting or procuring an espionage offence or making it easier to do so

856. Section 91.11 will make it an offence to solicit or procure an espionage offence, or make it easier for a person to do so. The offence will apply where a person engages in conduct in relation to another person (the target), with the intention of soliciting or procuring, or making it easier to solicit or procure, the target to deal with information or a thing in a way that would constitute an offence against Subdivision A (espionage) or B (espionage on behalf of foreign principals).

857. The offence will be punishable by a maximum of 15 years imprisonment.

858. An example of this offence is as follows. Person C is employed by a foreign intelligence service undertaking operations in Australia. Person A knows Person D is an employee of a commonwealth department and believes that Person C has access to highly classified information. Person C joins Person D's soccer team and establishes a personal relationship with Person D. Person C does so with the intention of procuring or soliciting Person D to provide classified information at some future date.

859. The purpose of this offence is to address gaps in the current law, which does not criminalise soliciting or procuring espionage. This offence will give law enforcement the means to deal with this conduct at the time it occurs, without the need to wait until an espionage offence is committed or sensitive information is actually passed to a foreign principal.

860. To establish this offence the prosecution will need to prove beyond reasonable doubt that:

- a person intentionally engages in conduct in relation to another person (the target)
- the person engages in the conduct with the intention of soliciting or procuring, or making it easier to solicit or procure, the target to commit an offence against Subdivision A (espionage) or Subdivision B (espionage on behalf of foreign principals), and
- the:
    - person engaged in the conduct on behalf of a foreign principal

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

and the person is reckless as to this element.

861. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 91.11(1)(a). Under subsection 5.2(1) of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

862. For paragraph 91.11(1)(a), the prosecution will have to prove beyond a reasonable doubt that the defendant intentionally engaged in conduct in relation to another person (the target). Consistent with subsection 4.1(2) of the Criminal Code, the reference to 'engages in conduct' in paragraph 91.11(1)(a) means to do an act or to omit to perform an act.

863. For paragraph 91.11(1)(b), the prosecution will have to prove beyond reasonable doubt that the defendant engaged in the relevant conduct intending to solicit or procure, or make it easier to solicit of procure, the target to deal with information or a thing in a way that would constitute an offence against Subdivision A (espionage) or B (espionage on behalf of foreign principals).

864. Subdivisions A and B create the following offences:

- Espionage – dealing with information etc. concerning national security which is or will be made available to a foreign principal (section 91.1)
- Espionage – dealing with information etc. which is or will be made available to a foreign principal (section 91.2)
- Espionage – security classified information etc. (section 91.3), and
- Espionage on behalf of a foreign principal (section 91.11).

865. The offence is intended to criminalise the procuring or soliciting conduct itself. Therefore, it will not be necessary for the prosecution to prove that the target actually deals with information in a manner that would constitute an offence against Subdivision A (espionage) or Subdivision B (espionage on behalf of foreign principals), only that the defendant intended that their conduct would solicit or procure, or make it easier to solicit or procure, the target to do so.

866. The term 'solicits' will take its ordinary meaning and is intended to include asking for, requesting, pressing for, or trying to obtain information or a thing from another person.

867. The term 'procure' is defined in the Dictionary to the Criminal Code in the context of sexual activity offences to mean:

- encourage, entice or recruit the person to engage in that activity, or
- induce the person (whether by threats, promises or otherwise) to engage in that activity.

868. Although this definition is limited to sexual activity offences, it is intended that the term *procure* in section 91.11 will be interpreted consistently with the definition in the Dictionary. This meaning is also appropriate in the context of procuring espionage and would cover a situation where, for example, an agent from a foreign intelligence service induces a target to commit an espionage offence by promising to pay money or provide another benefit.

869. Paragraph 91.11(1)(b) also captures conduct intended to 'make it easier' to solicit or procure espionage. This is intended to capture behaviour such as cultivating or grooming a target before the attempt to solicit or procure espionage is made. For example, a person may arrange meetings, provide gifts, or seek to establish a relationship of trust or friendship with a target. It would also include seeking passage of an unclassified government document or informed comment with the intent of procuring or soliciting the target to provide classified information in the future.

870. Paragraph 91.11(1)(b) contains the fundamental component of the offence – the prosecution must prove that the person actually intended to solicit or procure the target to engage in an espionage offence. It would not be sufficient to show that the person's conduct was of a nature that was merely suggestive of that intent.

871. In the example above, Person C has joined the same soccer team and established a friendship with Person D, intending to make it easier to solicit or procure Person D to commit an espionage offence in the future.

872. For paragraph 91.11(1)(c), the prosecution will have to prove beyond a reasonable doubt that the defendant's conduct was engaged in on behalf of, or in collaboration with, a foreign principal, on behalf of a person acting on behalf of a foreign principal, directed, funded or supervised by a foreign principal or a person acting on behalf of a foreign principal. Recklessness is the fault element for this element. Therefore, the defendant must have been aware of a substantial risk that his or her conduct was engaged in on behalf of, or in collaboration with, a foreign principal, on behalf of a person acting on behalf of a foreign principal, directed, funded or supervised by a foreign principal or a person acting on behalf of a foreign principal and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk.

873. It is possible that a defendant will know, or be reckless, as to the fact that they are engaging in conduct a foreign government because they are being tasked by a person who identifies himself or herself as an official of a foreign government. In this case, the person will be engaging in the conduct on behalf of the foreign principal.

874. However, it may also be the case that the defendant is not tasked directly by a foreign government official, but by an intermediary. In this case, the prosecution will have to prove beyond a reasonable doubt that the defendant was aware of a substantial risk that he or she

was being tasked by a person acting on behalf of a foreign principal and that it was unjustifiable to take that risk. This may be the case where, for example, the intermediary advises the defendant that the intermediary acts in coordination with foreign officials, or the intermediary facilitates preferential treatment for the defendant from a foreign government.

875. Consistent with subsection 91.11(2), for the purposes of paragraph 91.11(1)(c), the person does not need to have in mind a particular foreign country and may have in mind more than one foreign country. For example, a defendant may assist an individual who has identified themselves to the defendant as a foreign official, but has not specified which foreign country they represent. Or, a defendant may provide assistance in the knowledge this assistance will or could assist multiple foreign principals at the same time.

876. Section 91.11(3) provides that a person may still be found guilty of an offence against subsection 91.11(1):

- even if an offence against Subdivision A or B is not committed (paragraph 91.11(3)(a))
- even if it is impossible for the target to deal with the information or thing in a way that would constitute an offence against Subdivision A or B (paragraph 91.11(3)(b))
- even if the person does not have in mind particular information or a particular thing or a particular dealing or kind of dealing with the information or thing, at the time the person engages in conduct in relation to the target (paragraph 91.11(3)(c)), or
- whether or not it is a single dealing, or multiple dealings that the person intends to solicit or procure or make it easier to procure (paragraph 91.11(3)(d)).

877. Paragraph 91.11(3)(a) and (b) are consistent with the fundamental intention of the offence – to criminalise the person's intention to procure or solicit the target to engage in an espionage offence. Therefore, it will not matter if no offence is actually committed, or it is impossible for the offence to take place.

878. Section 91.11(3)(c) and (d) accommodate for the wide range of activity and techniques that the practice of soliciting or procuring espionage encompasses. It is possible that when the offender makes contact with a target the offender will not have particular information or a thing, or a particular kind of dealing with the information or thing, in mind. For example, the offender may only know that the target is well connected to government or that the target has access to classified information, without knowing exactly what information the target can provide. Further, there is no fixed pattern for how an offender will approach a target. In some instances the offender will meet the target and solicit information in one dealing. In other instances, the offender may build a relationship of trust with the target through multiple dealings, and intends to build up to inducing the target to commit espionage.

879. Subsection 91.11(4) specifies that section 11.1(attempt) does not apply to an offence against subsection 91.11(1). Section 11.1 of the Criminal Code extends criminal responsibility for all Commonwealth offences and operates to automatically provide for ancillary offences such as attempting to commit an offence or inciting the commission of an

offence. Subsection 91.11(4) modifies the automatic application of section 11.1 in relation to the ancillary offence of attempt. This is appropriate because the offence is already directed at conduct that is preparatory in nature.

880. The maximum penalty of 15 years imprisonment is comparable with the maximum penalties for Criminal Code offences of procuring a child to engage in sexual activity outside Australia (section 272.14) and 'grooming' a child to engage in sexual activity outside Australia(section 272.15), which also carry maximum penalties of 15 years imprisonment. The maximum penalty is appropriate to deter and punish the activity of soliciting or procuring espionage in Australia. The serious harm that can flow from such activities warrants a significant penalty, especially if a foreign principal is successful in obtaining classified information that will prejudice Australia's national security.

Section 91.12 – Offence of preparing for an espionage offence

881. Section 91.12 will make it an offence to prepare for or plan an espionage offence. The new offence will criminalise conduct in preparation for, or planning, an offence of espionage, or espionage on behalf of foreign principals. The offence will be punishable by a maximum penalty of 15 years imprisonment.

882. Examples of this offence could include:

- Example 1: Person A seeks access to a secure network that contains classified materials including national security information, at the direction of Person B, a foreign national. Person A has not yet located or determined a particular document, or documents, to obtain and pass on to Person B.

- Example 2: Person D installs malware onto the phones of Australian government officials with the intent to listen to classified conversations and pass on information to Person E, who works for a foreign government.

883. The purpose of the offence is to give law enforcement authorities the means to deal with preparatory conduct and enable a person to be arrested before any without the need to wait until an espionage offence is committed or sensitive information is actually passed to a foreign principal.

884. To establish the offence, prosecution will need to prove beyond a reasonable doubt that:

- a person intentionally engages in conduct, and

- the person does so with the intention of preparing for, or planning, an offence against Subdivision A (espionage) or B (espionage on behalf of foreign principals).

885. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 91.12(1)(a). Under section 5.2 of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct. Consistent with subsection 4.1(2) of the Criminal Code, the reference to 'engages in conduct' in paragraph 91.12(1)(a) means to do an act or to omit to perform an act.

886. For paragraph 91.12(1)(b), the prosecution will have to prove beyond a reasonable doubt that the person engages in conduct with the intention of preparing for, or planning, an offence against Subdivision A (espionage) or B (espionage on behalf of foreign principals). The terms preparation and planning are not defined and are intended to take their ordinary meanings.

- The term 'preparation' could include acts to conceive, formulate, make ready, arrange, and assemble an idea, plan, thing, or person for an offence against Subdivision A (espionage) or B (espionage on behalf of foreign principals).

- The term 'planning' could include acts to organise, arrange, design, draft, or setup an idea, plan, thing, or person for an offence against Subdivision A (espionage) or B (espionage on behalf of foreign principals).

887. Given the offences are directed at behaviour at the planning or planning stage, it is appropriate to impose the fault element of intention on both of the elements of the offence. This will ensure that a person will only be guilty of this offence where there is sufficient evidence that the person intended to prepare for, or plan, an espionage offence.

888. The maximum penalty for this offence is 15 years imprisonment. While persons who attempt to commit offences are generally subject to the same penalty as if the actual offence had been carried out, the offence at section 91.12 is intended to capture behaviour at the planning stage, rather than the more advanced stage at which an ancillary offence of attempt could otherwise apply.

889. Subsection 91.12(2) specifies that section 11.1(attempt) does not apply to an offence against subsection 91.12(1). Section 11.1 of the Criminal Code extends criminal responsibility for all Commonwealth offences and operates to automatically provide for ancillary offences such as attempting to commit an offence or inciting the commission of an offence. Subsection 91.12(2) modifies the automatic application of section 11.1 in relation to the ancillary offence of attempt. This is appropriate because the offence is already directed at conduct that is preparatory in nature.

890. Under paragraph 91.12(3)(a), the preparatory offence at subsection 91.12(1) will apply whether or not an offence against Subdivision A or B is actually committed. This is consistent with the intention behind the offence to allow intervention by law enforcement prior to an act of espionage occurring.

891. Under paragraph 91.12(3)(b), the preparatory offence in subsection 91.12(1) will apply whether or not the person engages in conduct in preparation for, or planning, a specific offence against a provision of Subdivision A or B. This clarifies that it is not necessary for the prosecution to identify a specific offence. It will be sufficient for the prosecution to prove that the particular conduct was related to 'an' offence. This ensures that the offence will be available where a person has planned a range of activities preparatory to committing an espionage offence that are still in the formative stages. For example, where a person has not necessarily decided on a particular document to pass to a foreign principal, or where a person has made arrangements to provide a particular document to a foreign principal and has taken steps, but has not yet obtained a copy of the document.

892. Under paragraph 91.12(3)(c), the preparatory offence at subsection 91.12(1) will apply whether or not the act is done in preparation for, or planning, more than one offence against a provision of Subdivision A or B. This clarifies that the offence will still apply where a person has engaged in preparatory conduct in relation to several offences against Subdivision A or B.

Section 91.13 – Defences

893. The general defences available under Part 2.3 of the Criminal Code will be available to a person accused of an offence under Subdivision C. In addition, section 91.13 creates the following specific defences:

- the person dealt with the information or article in accordance with a law of the Commonwealth
- the person dealt with the information or article in accordance with an arrangement or agreement to which the Commonwealth is party and which allows for the exchange of information or articles, or
- the person dealt with the information or article in the person's capacity as a public official.

894. The offences in Subdivision B are only intended to apply where a person's dealing with information is not a proper or legitimate part of their work. There are a vast range of legitimate circumstances in which public officials deal with information concerning Australia's national security (including highly classified information) in performing their duties. For example, possessing or copying information concerning national security is a day to day occurrence in many Commonwealth departments and agencies and for Ministers and their staff. It is not intended to criminalise these dealings.

895. Paragraph 91.13(1)(a) creates a defence to a prosecution for an offence against Subdivision B that the person dealt with the information or article in accordance with the law of the Commonwealth.

896. 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 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, section 91.13(1) casts the matter of lawful authority as a defence, which has the effect of placing an evidentiary burden of proof on the defendant.

897. If lawful authority was an element of the espionage offences in Subdivision C, 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 thing in the relevant manner. This is a significant barrier to prosecutions.

898. 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.

899. Consistent with section 13.3 of the Criminal Code, in the case of an evidential burden, the defendant bears the burden of adducing or pointing to evidence that suggests a reasonable possibility that the matter exists or does not exist. If the defendant discharges an evidential burden, the prosecution must disprove those matters beyond reasonable doubt, consistent with section 13.1 of the Criminal Code.

900. Section 10.5 of the Criminal Code provides a general defence of lawful authority applicable to all Commonwealth offences. This defence is narrow and only applies to conduct that is specifically justified or excused by a law. Consistent with the definition of ***law*** in the Dictionary to the Criminal Code, this means the conduct must be specifically justified or excused by a law of the Commonwealth.

901. The defence at paragraph 91.13(1)(a) is broader than the lawful authority defence available under section 10.5 and will cover a person acting 'in accordance' with a law of the Commonwealth, rather than the law of the Commonwealth needing to specifically justify or excuse the person's conduct.

902. Paragraph 91.13(1)(b) creates a defence to a prosecution for an offence against Subdivision B that the person dealt with the information or article in accordance with an agreement or arrangement to which the Commonwealth is party which allows for the exchange of information or things. Many departments and agencies share information with international counterparts as part of their normal business dealings. Often this information is highly sensitive and highly classified. This defence provides that the espionage offences in Subdivision B do not apply if a person was sharing information or things in accordance with an agreement or arrangement to which the Commonwealth was a party and which allows for the exchange of information or articles.

903. The terms 'arrangement' and 'agreement' are not defined and will be given their ordinary meaning. The term 'agreement' is not intended to be limited by the meaning of 'agreement' in Australian international practice as being a treaty, nor is it intended to require evidence of a formal contractual or legal agreement. It is intended that such terms will capture agreements or arrangements in a range of forms, including those made by exchange of letters or as a memorandum of understanding.

904. The defence at paragraph 91.13(1)(c) applies when a person dealt with the information or thing in the person's capacity as a public official. ***Public official*** is defined in the Dictionary to the Criminal Code to include:

- a Commonwealth public official
- an officer or employee of the Commonwealth or of a State or Territory
- an individual who performs work for the Commonwealth, or for a State or Territory, under a contract
- an individual who holds or performs the duties of an office established by a law of the Commonwealth or of a State or Territory

- an individual who is otherwise in the service of the Commonwealth or of a State or Territory (including service as a member of a military force or police force)
- a member of the executive, judiciary or magistracy of the Commonwealth or of a State or Territory, and
- an officer or employee of:
- an authority of the Commonwealth, or
- an authority of a State or Territory.

905. Commonwealth ***public official*** is defined in the Dictionary to the Criminal Code to mean:

- the Governor-General
- a person appointed to administer the Government of the Commonwealth under section 4 of the Constitution
- a Parliamentary Secretary
- a member of either House of the Parliament
- an individual who holds an appointment under section 67 of the Constitution
- the Administrator, an Acting Administrator, or a Deputy Administrator, of the Northern Territory
- a Commonwealth judicial officer (as defined in the Dictionary to the Criminal Code)
- an APS employee
- an individual employed by the Commonwealth other than under the *Public Service Act 1999*
- a member of the Australian Defence Force
- a member or special member of the AFP
- an individual (other than an official of a registered industrial organisation) who holds or performs the duties of an office established by or under a law of the Commonwealth, other than:
    - the Corporations (Aboriginal and Torres Strait Islander) Act 2006
    - the Australian Capital Territory (Self-Government) Act 1988
    - the Corporations Act 2001

    - the Norfolk Island Act 1979, or
    - the Northern *Territory (Self-Government) Act 1978*
- an officer or employee of a Commonwealth authority
- an individual who is a contracted service provider for a Commonwealth contract
- an individual who is an officer or employee of a contracted service provider for a Commonwealth contract and who provides services for the purposes (whether direct or indirect) of the Commonwealth contract
- an individual (other than an official of a registered industrial organisation) who exercises powers, or performs functions, conferred on the person by or under a law of the Commonwealth, other than:
    - the Corporations (Aboriginal and Torres Strait Islander) Act 2006
    - the Australian Capital Territory (Self-Government) Act 1988
    - the Corporations Act 2001
    - the Norfolk Island Act 1979
    - the Northern *Territory (Self-Government) Act 1978*, or
- a provision specified in the regulations
- an individual who exercises powers, or performs functions, conferred on the person under a law in force in the Territory of Christmas Island or the Territory of Cocos (Keeling) Islands (whether the law is a law of the Commonwealth or a law of the Territory concerned), or
- the Registrar, or a Deputy Registrar, of Aboriginal and Torres Strait Islander Corporations.

906. This defence is intended to apply where a person discloses information in the person's capacity as a public official. This may include, for example, an employee duty statement, a policy guidance document or employee practice manual, or previous examples of the same conduct which has been authorised by superiors. It will not be a defence to a charge of espionage where a person has gone beyond their ordinary duties.

907. Note 1 under the defence at subsection 91.13(1) clarifies that the defendant will bear an evidentiary burden in relation to this defence. Consistent with section 13.3 of the Criminal Code, the defendant will need to point to evidence that suggests a reasonable possibility that the defence is made out. If this is done, the prosecution must refute the defence beyond reasonable doubt (section 13.1).

908. Both AFP and CDPP consider the availability of any defences when considering whether to investigate and prosecute criminal offences. In relation to prosecution decisions, the Prosecution Policy of the Commonwealth specifically requires the CDPP to take into

account any lines of defence which are plainly open to, or have been indicated by, the alleged offender in deciding whether there is a reasonable prospect of a conviction being secured. Subsection 93.1 (to be inserted by Item 18 of Schedule 1) requires the Attorney-General consider whether the defendant's conduct is authorised under the defences in section 91.13 before providing his or her consent to the institution of proceedings for the commitment of a person for trial for an offence to which the defence applies.

909. Note 1 under the defence at subsection 91.9(1) clarifies that the defendant will bear an evidentiary burden in relation to this offence. This is appropriate because the defendant should be readily able to point to evidence that they acquired the relevant information or thing indirectly from a publically available source. Consistent with section 13.3 of the Criminal Code, the defendant will need to point to evidence that suggests a reasonable possibility that the defence is made out. If this is done, the prosecution must refute the defence beyond reasonable doubt (section 13.1).

Section 91.14 – Geographical jurisdiction

910. Section 91.14 will apply Section 15.4 (extended geographical jurisdiction—Category D) to each offence against Subdivision C

911. Under section 15.4, the effect of Category D geographical jurisdiction is that each offences against Subdivision C applies:

- whether or not the conduct constituting the alleged offence occurs in Australia, and
- whether or not a result of the conduct constituting the alleged offence occurs in Australia.

912. Category D geographical jurisdiction is appropriate because intelligence agencies may undertake key facets of espionage activities against Australia in foreign countries to conceal these activities from relevant authorities seeking to prevent these activities. For example, an official from Country X may establish contact with Australian Person Y while on official travel in Country Z, and obtain Person Y's agreement to conduct espionage on their return to Australia.

Division 92 – Foreign interference

Subdivision A – Preliminary

Section 92.1 – Definitions

913. New section 92.1 inserts definitions relevant to the foreign interference offences in Division 92.

914. ***Deception*** is defined to mean an intentional or reckless deception, whether by words or other conduct, and whether as to fact or as to law, and includes:

- a deception as to the intentions of the person using the deception or any other person, and

- conduct by a person that causes a computer, a machine or an electronic device to make a response that the person is not authorised to cause it to do.

915. This definition is consistent with the definition in section 133.1 of the Criminal Code which applies to Commonwealth fraud offences. The definition is explicit about the fault elements for deception, which may be intentional or reckless. The definition also takes into account the deception of computers, machines or electronic devices which is necessary given the pervasive nature of information technology for transactions and communications.

916. ***Menaces*** is defined to have the same meaning as in Part 7.5 of the Criminal Code, which relates to unwarranted menaces (also known as blackmail).

917. Section 138.2 of the Criminal Code defines menaces as including:

- a threat (whether express or implied) of conduct that is detrimental or unpleasant to another person, or

- a general threat of detrimental or unpleasant conduct that is implied because of the status, office or position of the maker of the threat.

918. Subsection 138.2(2) provides that a threat against an individual is taken not to be menaces unless:

- both:

    - the threat would be likely to cause the individual to act unwillingly, and

    - the maker of the threat is aware of the vulnerability of the individual to the threat, or

- the threat would be likely to cause a person of normal stability and courage to act unwillingly.

919. For example, a demand for payment accompanied by a threat to sue to recover the debt would not be considered menaces, because it suing to enforce a debt is a proper means of enforcing the demand. However, a demand for information accompanied by a threat to disclose private information about a person's marital affair that would jeopardise a person's family could qualify as menaces as it could make a person of normal stability and courage act unwillingly.

Subdivision B – Foreign interference

Section 92.2 – Offence of intentional foreign interference

920. Section 92.2 creates two offences of intentional foreign interference.

Interference generally

921. Subsection 92.2(1) will make it an offence to engage in conduct that is covert or involves deception, threats or menaces on behalf of a foreign principal with an intention to:

- influence a political or governmental process of the Commonwealth or a State or Territory
- influence the exercise of an Australian democratic or political right
- support intelligence activities of a foreign principal, or
- prejudice Australia's national security.

922. This offence will be punishable by a maximum penalty of 20 years imprisonment.

923. An example of this offence is as follows. Person A is an Australia-based intermediary who responds to direction from officers from the government of Country B, in return for payment. Country B officials task Person A to obtain classified information from Commonwealth government departments to support the intelligence priorities of Country B. Person A undertakes several activities to further this goal, including identifying people who work in the relevant departments, providing these details to Country B officials, and seeking to form relationships with these Commonwealth department employees. Person A misleads these Commonwealth department employees about the nature of Person A's employment and the fact they are pursuing these relationships at the direction and supervision of Country B, for intelligence purposes. Person A also takes steps to conceal their contact with officials from Country B, using encrypted messaging applications.

924. To establish this offence, the prosecution will need to prove beyond a reasonable doubt that:

- a person intentionally engaged in conduct
- the:
    - person engaged in the conduct on behalf of a foreign principal
    - person engaged in the conduct on behalf of a person acting on behalf of a foreign principal
    - person engaged in the conduct in collaboration with a foreign principal
    - person engaged in the conduct in collaboration with a person acting on behalf of a foreign principal
    - conduct was directed, funded or supervised by a foreign principal, or
    - conduct was directed, funded or supervised by a person acting on behalf of a foreign principal

  and the person is reckless as to this element.
- the person intends that their conduct will:
    - influence a political or governmental process of the Commonwealth or a State or Territory

- influence the exercise, whether or not in Australia, of an Australian democratic or political right
- support intelligence activities of a foreign principal, or
- prejudice Australia's national security, and

- any part of the conduct:
  - is covert or involves deception
  - involves the person making a threat to cause serious harm, whether to the person to whom the threat is made or any other person, or
  - involves the person making a demand with menaces

  and the person is reckless as to this element.

925. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 92.2(1)(a). Intention will also apply to paragraph 92.2(1)(c). Under subsection 5.2(1) of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

926. Recklessness will be the fault element for paragraphs 92.2(1)(b) and (d). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and
- a result if he or she is 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 the risk.

927. For paragraph 92.2(1)(a) of the offence, the prosecution will have to prove beyond a reasonable doubt that the defendant intended to engage in the relevant conduct. Consistent with subsection 4.1(2) of the Criminal Code, the reference to 'engages in conduct' in paragraph 92.2(1)(a) means to do an act or to omit to perform an act.

928. For paragraph 92.2(1)(b), the prosecution will have to prove beyond a reasonable doubt that the defendant's conduct was engaged in on behalf of, or in collaboration with, a foreign principal, on behalf of a person acting on behalf of a foreign principal, directed, funded or supervised by a foreign principal or a person acting on behalf of a foreign principal. Recklessness is the fault element for this element. Therefore, the defendant must have been aware of a substantial risk that his or her conduct was engaged in on behalf of, or in collaboration with, a foreign principal, on behalf of a person acting on behalf of a foreign principal, directed, funded or supervised by a foreign principal or a person acting on behalf of a foreign principal and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk.

929. It is possible that a defendant will know, or be reckless, as to the fact that they are engaging in conduct a foreign principal because they are being tasked by a person who

identifies himself or herself as representing a foreign principal. In this case, the person will be engaging in the conduct on behalf of the foreign principal.

930. However, it may also be the case that the defendant is not tasked directly by a foreign government official, but by an intermediary. In this case, the prosecution will have to prove beyond a reasonable doubt that the defendant was aware of a substantial risk that he or she was being tasked by a person acting on behalf of a foreign principal and that it was unjustifiable to take that risk. This may be the case where, for example, the intermediary advises the defendant that the intermediary acts in coordination with foreign officials, or the intermediary facilitates preferential treatment for the defendant from a foreign government.

931. Consistent with subsection 92.2(3), for the purposes of paragraph 92.1(1)(b), the person will not need to have in mind a particular foreign principal and may have in mind more than one foreign principal. For example, a defendant may assist an individual who has identified themselves to the defendant as a foreign official, but has not specified which foreign country they represent. Or, a defendant may provide assistance in the knowledge this assistance will or could assist multiple foreign principals at the same time.

932. For the purposes of paragraph 92.2(1)(c), the prosecution will have to prove beyond a reasonable doubt that the person intended that his or her conduct would:

- influence a political or governmental process of the Commonwealth or a State or Territory (subparagraph 92.2(1)(c)(i))
- influence the exercise, whether or not in Australia, of an Australian democratic or political right (subparagraph 92.2(1)(c)(ii))
- support intelligence activities of a foreign principal (subparagraph 92.2(1)(c)(iii)), or
- prejudice Australia's national security (subparagraph 92.2(1)(c)(iv))

933. Subparagraph 92.2(1)(c)(i) refers to a political or governmental process of the Commonwealth or a State or Territory. The reference to political processes is intended to cover matters within political parties (such as which candidate is pre-selected or the manner in which preferences are to be allocated at an election) as well as political matters within the parliamentary process (such as decisions by shadow Cabinet or decisions by political parties about policies). The reference to governmental processes is intended to cover decision making by the Executive Government, including Cabinet decisions, Executive Council decisions and decisions of individual ministers or departments. The term is intended to cover parliamentary processes such as votes on legislation and establishment and conduct of committees or inquiries.

934. Subparagraph 92.2(1)(c)(ii) refers to the exercise, whether or not in Australia, of Australian democratic or political rights. This term is intended to cover a broad range of rights held by Australians in relation to participation in Australia's democracy, including voting in elections and referenda and participating in lawful protests. The reference to 'whether or not in Australia' is intended to reflect the fact that Australia's can exercise Australian democratic rights from outside Australia. For example, this element is intended to be sufficiently broad to cover an Australian's right to vote in an Australian election while he or she is physically located outside Australia. The reference to 'Australian' democratic and

political rights is intended to limit the operation of this paragraph only to rights that arise because of a person's status as Australian. For example, it is not intended to cover a situation where a person is a joint citizen of Australia and the United Kingdom and has a right to vote in United Kingdom elections while physically located in Australia. This would be a United Kingdom democratic right, rather than an Australian democratic right, even though it is being exercised 'in' Australia.

935. Subparagraph 92.2(1)(c)(iii) refers to support for the intelligence activities of a foreign principal. Intelligence activities is intended to cover the full range of information gathering and facilitation activities pursued by foreign principals to obtain or collect information about capabilities, intentions, vulnerabilities or other activities of Australian governments, government agencies or people or organisations within Australia. This could include obtaining or collecting information about the identity, finances or activities of individuals, groups or other identities. The term 'intelligence activities' is also intended to cover traditional activities of intelligence agencies, including signals intelligence and geospatial and imagery intelligence.

936. Subparagraph 92.2(1)(iv) refers to prejudicing Australia's national security (as defined in section 90.4. The definition in section 90.4 covers a broad range of possible prejudice to Australia's national security, such as damage to Australia's defence operations or harm to Australia's international relations.

937. In the example above, Person A intends that their conduct will support the intelligence activities of the Country B, which would fall within the definition in subparagraph 92.2(1)(c)(iii).

938. For the purposes of paragraph 92.2(1)(d), the prosecution will have to prove beyond a reasonable doubt that any part of their conduct is covert or involves deception, involves the making of a threat to cause serious harm or involves a demand with menaces. Recklessness is the fault element for this element. Therefore, the defendant will have to be aware of a substantial risk that any part of their conduct is covert or involves deception, involves the making of a threat to cause serious harm or involves a demand with menaces and that, having regard to the circumstances known to him or her that it is unjustifiable to take that risk.

939. Subparagraph 92.2(1)(d)(i) refers to any part of the conduct being covert or involving deception. The reference to 'covert' is intended to cover any conduct that is hidden or secret, or lacking transparency. For example, conduct may be covert if a person takes steps to conceal their communications with the foreign principal, such as deliberately moving onto encrypted communication platforms when dealing with the foreign principal, meeting in a concealed location, communicating by coded messages, or leaving communications in a concealed location for collection by the foreign principal. Conduct may also be covert if the defendant copies documents or listens into private conversations without the targeted person's knowledge or consent, and then passes that information to a foreign principal.

940. Subparagraph 92.2(1)(d)(i) refers to ***deception***, which section 92.1 defines to mean an intentional or reckless deception, whether by words or other conduct, and whether as to fact or as to law, and includes:

- a deception as to the intentions of the person using the deception or any other person, and

- conduct by a person that causes a computer, a machine or an electronic device to make a response that the person is not authorised to cause it to do.

941. The reference to conduct 'involving deception' is intended to cover conduct that seeks to cause someone to accept as true or valid what is false or invalid. This would include a person telling lies or misleading a person. In the context of this offence, this may include a person lying about their employment with a foreign government or saying that the information is not intended for passage to a foreign principal.

942. Subparagraph 92.2(1)(d)(ii) refers to a person making a threat to cause serious harm, whether to the person to whom the threat is made or any other person. ***Threat*** is defined in the Dictionary to the Criminal Code as including a threat made by any conduct, whether express or implied and whether conditional or unconditional. ***Serious harm*** is defined in the Dictionary to the Criminal Code as meaning harm (including the cumulative effect of any harm):

- that endangers, or is likely to endanger, a person's life, or
- that is, or is likely to be significant and longstanding.

943. ***Harm*** is defined in the Dictionary to the Criminal Code as meaning physical harm or harm to a person's mental health, whether temporary or permanent. However, it does not include being subjected to any force or impact that is within the limits of what is acceptable as incidental to social interaction or to life in the community. ***Harm to a person's mental health*** is defined in the Dictionary to the Criminal Code as including significant psychological harm, but does not include mere ordinary emotional reactions such as those of only distress, grief, fear or anger.

944. For subparagraph 92.2(1)(d)(ii) to apply, the defendant must be the person making the threat The subparagraph applies where:

- the defendant (Person A) makes a threat to Person B and the threat is that serious harm will be caused to Person B, or
- the defendant (Person A) makes a threat to Person B and the threat is that serious harm will be caused to Person C.

945. It is necessary to cover both of these scenarios because foreign interference activities, particularly those undertaken on behalf of foreign governments, can involve interference with the activities or rights of diaspora or expatriate communities in Australia. For example, a person acting on behalf of Country X might seek to coercively direct the activities of Australia-based Person Y (whose family originates from Country X) by threatening that, if Person Y does not comply with Country X's wishes, serious harm will be caused to Person Y's family members who are still living in Country X.

946. Subparagraph 92.2(1)(d)(iii) refers a person making a demand with menaces. Consistent with the definition of ***menaces*** in section 92.1, the term has the same meaning as in Part 7.5 of the Criminal Code. ***Menaces*** is defined in section 138.2 of the Criminal Code as including a threat (as defined in the Dictionary to the Criminal Code), whether express or implied, of conduct that is detrimental or unpleasant to another person, or a general threat of

detrimental or unpleasant conduct that is implied because of the status, office or position of the maker of the threat. A threat against an individual is taken not the be menaces unless:

- the threat would be likely to cause the individual to act unwillingly and the maker of the threat is aware of the vulnerability of the individual to the threat, or
- the threat would be likely to cause a person of normal stability and courage to act unwillingly.

947. Under subsection 138.2(3), a threat against a person who is not an individual is taken not to be menaces unless the threat would ordinarily cause an unwilling response, or the threat would be likely to cause an unwilling response because of a particular vulnerability of which the maker of the threat is aware.

948. Subparagraph 92.2(1)(d)(iii) is intended to capture threats that would generally be considered to be blackmail, rather than the threats to cause serious physical or mental harm covered by subparagraph 92.2(1)(d)(ii). For subparagraph 92.2(1)(d)(iii), the defendant must be the person making the demand with menaces.

949. Examples of demands with menaces would include:

- a threat to arrest the targeted person upon their entry to another country,
- a threat to bankrupt a business associated with a targeted person, or
- a threat to ensure the targeted person (or one of their family members) is denied a visa for entry to another country.

950. In the example above, Person A would be aware of a substantial risk that their conduct is covert (because Person A is deliberately using an encrypted messaging application in order to hide their communications with Country B). Person A would also be aware of a substantial risk that their conduct involves deception because they are telling lies and providing misleading information about their employment and reason for being in Australia.

951. The maximum penalty for the offence in subsection 92.2(1) is 20 years imprisonment. The commission of this offence would have serious consequences for the sovereignty of Australia. It is unacceptable for foreign principals to seek to influence or intimidate Australians or Australian governments, or pursue their intelligence activities, in a manner that is covert or deceptive or involves threats to cause serious harm or demands with menaces. In the worst case scenario, Australians could be threatened with death by a person acting on behalf of a foreign principal and intending to harm Australia's national security. This justifies the serious maximum penalty for the offence.

952. The Note to subsection 92.2(1) specifies that an alternative verdict may be available for an offence against subsection 92.2(1) in accordance with section 93.5.

Interference involving targeted person

953. Subsection 92.2(2) will make it an offence to engage in conduct on behalf of a foreign principal with an intention to influence another person (the target) in relation to a political or

governmental process or the exercise of an Australian democratic or political right without disclosing to the target that they are working for a foreign principal.

954. This offence will be punishable by a maximum penalty of 20 years imprisonment.

955. An example of this offence is as follows. Person C is an Australian citizen who undertakes activities for Country D in Australia in exchange for payment. Person C is specifically tasked by Country D officials to convince an Australian political party to change its policy to support free trade with Country D. Person C meets with senior party leaders to discuss this policy. In those meetings, Person C represents herself purely as an Australian citizen and does not disclose her relationship with Country D or the fact that her activities are undertaken on behalf of Country D.

956. To establish this offence, the prosecution will need to prove beyond a reasonable doubt that:

- a person intentionally engaged in conduct
- the:
    - person engaged in the conduct on behalf of a foreign principal
    - person engaged in the conduct on behalf of a person acting on behalf of a foreign principal
    - person engaged in the conduct in collaboration with a foreign principal
    - person engaged in the conduct in collaboration with a person acting on behalf of a foreign principal
    - conduct was directed, funded or supervised by a foreign principal, or
    - conduct was directed, funded or supervised by a person acting on behalf of a foreign principal

  and the person is reckless as to this element.
- the person intends that their conduct will influence another person (the target):
    - in relation to a political or governmental process of the Commonwealth or a State or Territory, or
    - in the target's exercise, whether or not in Australia, of an Australian democratic or political right, and
- the person intentionally conceals from, or fails to disclose to, the target the fact that their conduct was:
    - on behalf of a foreign principal
    - on behalf of a person acting on behalf of a foreign principal

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

957. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraphs 92.2(2)(a) and (d). Intention also applies to paragraph 92.2(2)(c). Under subsection 5.2(1) of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

958. Recklessness is the fault element for paragraph 92.2(2)(b). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and
- a result if he or she is 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 the risk.

959. For paragraph 92.2(2)(a) of the offence, the prosecution will have to prove beyond a reasonable doubt that the defendant intended to engage in the relevant conduct. Consistent with subsection 4.1(2) of the Criminal Code, the reference to 'engages in conduct' in paragraph 92.2(2)(a) means to do an act or to omit to perform an act.

960. For paragraph 92.2(2)(b), the prosecution will have to prove beyond a reasonable doubt that the defendant's conduct was engaged in on behalf of, or in collaboration with, a foreign principal, on behalf of a person acting on behalf of a foreign principal, directed, funded or supervised by a foreign principal or a person acting on behalf of a foreign principal. Recklessness is the fault element for this element. Therefore, the defendant must have been aware of a substantial risk that his or her conduct was engaged in on behalf of, or in collaboration with, a foreign principal, on behalf of a person acting on behalf of a foreign principal, directed, funded or supervised by a foreign principal or a person acting on behalf of a foreign principal and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk.

961. It is possible that a defendant will know, or be reckless, as to the fact that they are engaging in conduct a foreign government because they are being tasked by a person who identifies himself or herself as an official of a foreign government. In this case, the person will be engaging in the conduct on behalf of the foreign principal.

962. However, it may also be the case that the defendant is not tasked directly by a foreign government official, but by an intermediary. In this case, the prosecution will have to prove beyond a reasonable doubt that the defendant was aware of a substantial risk that he or she was being tasked by a person acting on behalf of a foreign principal and that it was unjustifiable to take that risk. This may be the case where, for example, the intermediary

advises the defendant that the intermediary acts in coordination with or provides advice to foreign officials, or the intermediary facilitates preferential treatment for the defendant from a foreign government.

963. Consistent with subsection 92.2(3), for the purposes of paragraph 92.2(1)(b), the person will not need to have in mind a particular foreign principal and may have in mind more than one foreign principal. For example, a defendant may assist an individual who has identified themselves to the defendant as a foreign official, but has not specified which foreign country they represent. Or, a defendant may provide assistance in the knowledge this assistance will or could assist multiple foreign principals at the same time.

964. For the purposes of paragraph 92.2(2)(c), the prosecution will have to prove beyond a reasonable doubt that the person intended for their act or omission to influence another person (the target):

- in relation to a political or governmental process of the Commonwealth or a State or Territory (subparagraph 92.2(2)(c)(i)), or

- in the target's exercise, whether or not in Australia, of an Australian democratic or political right (subparagraph 92.2(1)(c)(ii)).

965. Subparagraph 92.2(2)(c)(i) refers to a political or governmental process of the Commonwealth or a State or Territory. The reference to political processes is intended to cover matters within political parties (such as which candidate is pre-selected or the manner in which preferences are to be allocated at an election) as well as political matters within the parliamentary process (such as decisions by shadow Cabinet or decisions by political parties about policies). The reference to governmental processes is intended to cover decision making by the Executive Government, including Cabinet decisions, Executive Council decisions and decisions of individual ministers or departments. The term is intended to cover parliamentary processes such as votes on legislation and establishment and conduct of committees or inquiries.

966. Subparagraph 92.2(2)(c)(ii) refers to the exercise, whether or not in Australia, of Australian democratic or political rights. This term is intended to cover a broad range of rights held by Australians in relation to participation in Australia's democracy, including voting in elections and referenda and participating in lawful protests. The reference to 'whether or not in Australia' is intended to reflect the fact that Australia's can exercise Australian democratic rights from outside Australia. For example, this element is intended to be sufficiently broad to cover an Australian's right to vote in an Australian election while he or she is physically located outside Australia. The reference to 'Australian' democratic and political rights is intended to limit the operation of this paragraph only to rights that arise because of a person's status as Australian. For example, it is not intended to cover a situation where a person is a joint citizen of Australia and the United Kingdom and has a right to vote in United Kingdom elections while physically located in Australia. This would be a United Kingdom democratic right, rather than an Australian democratic right, even though it is being exercised 'in' Australia.

967. This offence is targeting undisclosed influence on another person in relation to one of the matters covered by subparagraphs 92.2(2)(c)(i) and (ii). Paragraph 92.2(2)(c) requires the defendant's conduct to be intended to influence another person (known as the target). For example, the defendant may, under direction from a foreign country, intentionally seek to

influence a Commonwealth Member of Parliament in relation to a pending vote in the House of Representatives. Another example would be where the defendant seeks to influence an Australian citizen as to how they should vote in a Federal election.

968. Whether or not this matter occurs or the conduct is capable of bringing it about is not relevant to the defendant's culpability for the offence. The defendant can still commit the offence despite the fact that the intended influence does not occur, or is not capable of occurring.

969. For the purposes of paragraph 92.2(2)(d), the prosecution will have to prove beyond a reasonable doubt that the defendant intentionally concealed from, or failed to disclose to, the target the fact that his or her conduct was engaged in on behalf of a foreign principal and that, having regard to the circumstances known to him or her, it is unjustifiable to take that risk.

970. For example, Person A is a prominent Australian citizen with strong connections to politics. Person A, acting at the direction of Country B, calls the Minister for Foreign Affairs arguing that Australia should adopt a policy favourable to Country B. In the call Person A does not disclose that she is representing Country B's views or is working on behalf of Country B. Person A has, for the purposes of paragraph 92.2(2)(d), failed to disclose the fact that she is engaging in conduct at the direction of a foreign principal.

971. The maximum penalty for the offence in subsection 92.2(2) is 20 years imprisonment. The commission of this offence would have serious consequences for the sovereignty of Australia. It is unacceptable for foreign principals to seek to influence Australians or Australian governments in relation to political or government processes or the exercise of Australian democratic or political rights. In the worst case scenario, a decision by the Cabinet or a minister with implications for national security could be influenced by a foreign principal without the Cabinet or minister's knowledge. This justifies the serious maximum penalty for the offence.

972. The Note to subsection 92.2(2) specifies that an alternative verdict may be available for offences against subsection 92.2(2) in accordance with section 93.5.

Section 92.3 – Offence of reckless foreign interference

973. Section 92.3 creates two offences of reckless foreign interference.

Interference generally

974. Subsection 92.3(1) will make it an offence to engage in conduct that is covert or involves deception, threats or menaces on behalf of a foreign principal where the person is reckless as to whether their conduct will:

- influence a political or governmental process of the Commonwealth or a State or Territory
- influence the exercise of an Australian democratic or political right
- support intelligence activities of a foreign principal, or
- cause harm to Australia's national security.

975. This offence will be punishable by a maximum penalty of 15 years imprisonment.

976. An example of this offence is as follows. Person E is an Australian citizen who undertakes activities in Australia at the direction of the intelligence agency of Country F. Country F seeks to suppress protests in Australia regarding a humanitarian crisis in Country F. Person E sends anonymous text messages to people in Australia involved in organising the protests threatening that serious harm will come to them if they continue their activities, and makes similar threats to protest organisers on social media. Person E is aware that the right to protest is an essential part of Australia's democratic processes.

977. To establish this offence, the prosecution will need to prove beyond a reasonable doubt that:

- a person intentionally engaged in conduct
- the:
    - person engaged in the conduct on behalf of a foreign principal
    - person engaged in the conduct on behalf of a person acting on behalf of a foreign principal
    - person engaged in the conduct in collaboration with a foreign principal
    - person engaged in the conduct in collaboration with a person acting on behalf of a foreign principal
    - conduct was directed, funded or supervised by a foreign principal, or
    - conduct was directed, funded or supervised by a person acting on behalf of a foreign principal

  and the person is reckless as to this element.
- the person was reckless as to whether his or her conduct would:
    - influence a political or governmental process of the Commonwealth or a State or Territory
    - influence the exercise, whether or not in Australia, of an Australian democratic or political right
    - support intelligence activities of a foreign principal, or
    - prejudice Australia's national security, and
- any part of the conduct:
    - is covert or involves deception

- involves the person making a threat to cause serious harm, whether to the person to whom the threat is made or any other person, or

- involves the person making a demand with menaces

and the person is reckless as to this element.

978. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 92.3(1)(a). Under subsection 5.2(1) of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

979. Recklessness is the fault element for paragraphs 92.3(1)(b), (c) and (d). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and

- a result if he or she is 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 the risk.

980. For paragraph 92.3(1)(a) of the offence, the prosecution will have to prove beyond a reasonable doubt that the defendant intended to engage in the relevant conduct. Consistent with subsection 4.1(2) of the Criminal Code, the reference to 'engages in conduct' in paragraph 92.3(1)(a) means to do an act or to omit to perform an act.

981. For paragraph 92.3(1)(b), the prosecution will have to prove beyond a reasonable doubt that the defendant's conduct was engaged in on behalf of, or in collaboration with, a foreign principal, on behalf of a person acting on behalf of a foreign principal, directed, funded or supervised by a foreign principal or a person acting on behalf of a foreign principal. Recklessness is the fault element for this element. Therefore, the defendant must have been aware of a substantial risk that his or her conduct was engaged in on behalf of, or in collaboration with, a foreign principal, on behalf of a person acting on behalf of a foreign principal, directed, funded or supervised by a foreign principal or a person acting on behalf of a foreign principal and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk.

982. It is possible that a defendant will know, or be reckless, as to the fact that they are engaging in conduct a foreign government because they are being tasked by a person who identifies himself or herself as an official of a foreign government. In this case, the person will be engaging in the conduct on behalf of the foreign principal.

983. However, it may also be the case that the defendant is not tasked directly by a foreign government official, but by an intermediary. In this case, the prosecution will have to prove beyond a reasonable doubt that the defendant was aware of a substantial risk that he or she was being tasked by a person acting on behalf of a foreign principal and that it was unjustifiable to take that risk. This may be the case where, for example, the intermediary advises the defendant that the intermediary acts in coordination with or provides advice to foreign officials, or the intermediary facilitates preferential treatment for the defendant from a foreign government.

984. Consistent with subsection 92.3(3), for the purposes of paragraph 92.3(1)(b), the person will not need to have in mind a particular foreign principal and may have in mind more than one foreign principal. For example, a defendant may assist an individual who has identified themselves to the defendant as a foreign official, but has not specified which foreign country they represent. Or, a defendant may provide assistance in the knowledge this assistance will or could assist multiple foreign principals at the same time.

985. For the purposes of paragraph 92.3(1)(c), the prosecution will have to prove beyond a reasonable doubt that the person was reckless as to whether their act or omission would:

- influence a political or governmental process of the Commonwealth or a State or Territory (subparagraph 92.3(1)(c)(i))
- influence the exercise, whether or not in Australia, of an Australian democratic or political right (subparagraph 92.3(1)(c)(ii))
- support intelligence activities of a foreign principal (subparagraph 92.3(1)(c)(iii)), or
- prejudice Australia's national security (subparagraph 92.3(1)(c)(iv))

986. Subparagraph 92.3(1)(c)(i) refers to a political or governmental process of the Commonwealth or a State or Territory. The reference to political processes is intended to cover matters within political parties (such as which candidate is pre-selected or the manner in which preferences are to be allocated at an election) as well as political matters within the parliamentary process (such as decisions by shadow Cabinet or decisions by political parties about policies). The reference to governmental processes is intended to cover decision making by the Executive Government, including Cabinet decisions, Executive Council decisions and decisions of individual ministers or departments. The term is intended to cover parliamentary processes such as votes on legislation and establishment and conduct of committees or inquiries.

987. Subparagraph 92.3(1)(c)(ii) refers to the exercise, whether or not in Australia, of Australian democratic or political rights. This term is intended to cover a broad range of rights held by Australians in relation to participation in Australia's democracy, including voting in elections and referenda and participating in lawful protests. The reference to 'whether or not in Australia' is intended to reflect the fact that Australia's can exercise Australian democratic rights from outside Australia. For example, this element is intended to be sufficiently broad to cover an Australian's right to vote in an Australian election while he or she is physically located outside Australia. The reference to 'Australian' democratic and political rights is intended to limit the operation of this paragraph only to rights that arise because of a person's status as Australian. For example, it is not intended to cover a situation where a person is a joint citizen of Australia and the United Kingdom and has a right to vote in United Kingdom elections while physically located in Australia. This would be a United Kingdom democratic right, rather than an Australian democratic right, even though it is being exercised 'in' Australia.

988. Subparagraph 92.3(1)(c)(iii) refers to support for the intelligence activities of a foreign principal. Intelligence activities is intended to cover the full range of information gathering and facilitation activities pursued by foreign principals to obtain or collect information about capabilities, intentions, vulnerabilities or other activities of

Australian governments, government agencies or people or organisations within Australia. This could include obtaining or collecting information about the identity, finances or activities of individuals, groups or other identities. The term 'intelligence activities' is also intended to cover traditional activities of intelligence agencies, including signals intelligence and geospatial and imagery intelligence.

989. Subparagraph 92.3(1)(iv) refers to prejudicing Australia's national security (as defined in section 90.4), which covers a broad range of possible prejudice to Australia's national security, such as damage to Australia's defence operations or harm to Australia's international relations.

990. In the example above, Person E would be aware of a substantial risk that their conduct would influence the exercise in Australia of an Australian democratic or political right, being the right to protest.

991. For the purposes of paragraph 92.3(1)(d), the prosecution will have to prove beyond a reasonable doubt that any part of their conduct is covert or involves deception, involves the making of a threat to cause serious harm or involves a demand with menaces. Recklessness is the fault element for this element. Therefore, the defendant will have to be aware of a substantial risk that any part of their conduct is covert or involves deception, involves the making of a threat to cause serious harm or involves a demand with menaces and that, having regard to the circumstances known to him or her that it is unjustifiable to take that risk.

992. Subparagraph 92.3(1)(d)(i) refers to any part of the conduct being covert or involving deception. The reference to 'covert' is intended to cover any conduct that is hidden or secret, or lacking transparency. For example, conduct may be covert if a person takes steps to mask or hide their communications with the foreign principal, such as deliberately moving onto encrypted communication platforms when dealing with the foreign principal, meeting in a concealed location, communicating by coded messages, or leaving communications in a concealed location for collection by the foreign principal. Conduct may also be covert if the defendant copies documents or listens into private conversations without the targeted person's knowledge or consent, and then passes that information to a foreign principal.

993. Subparagraph 92.3(1)(d)(i) refers to ***deception***, which section 92.1 defines to mean an intentional or reckless deception, whether by words or other conduct, and whether as to fact or as to law, and includes:

- a deception as to the intentions of the person using the deception or any other person, and

- conduct by a person that causes a computer, a machine or an electronic device to make a response that the person is not authorised to cause it to do.

994. The reference to conduct 'involving deception' is intended to cover conduct that seeks to cause someone to accept as true or valid what is false or invalid. This would include a person telling lies or misleading a person. In the context of this offence, this may include a person lying about their employment with a foreign government or that the information a person is seeking is intended for passage to a foreign principal.

995. Subparagraph 92.3(1)(d)(ii) refers to a person making a threat to cause serious harm, whether to the person to whom the threat is made or any other person. ***Threat*** is defined in

the Dictionary to the Criminal Code as including a threat made by any conduct, whether express or implied and whether conditional or unconditional. ***Serious harm*** is defined in the Dictionary to the Criminal Code as meaning harm (including the cumulative effect of any harm):

- that endangers, or is likely to endanger, a person's life, or
- that is, or is likely to be significant and longstanding.

996. ***Harm*** is defined in the Dictionary to the Criminal Code as meaning physical harm or harm to a person's mental health, whether temporary or permanent. However, it does not include being subjected to any force or impact that is within the limits of what is acceptable as incidental to social interaction or to life in the community. ***Harm to a person's mental health*** is defined in the Dictionary to the Criminal Code as including significant psychological harm, but does not include mere ordinary emotional reactions such as those of only distress, grief, fear or anger.

997. For subparagraph 92.3(1)(d)(ii) to apply, the defendant must be the person making the threat The subparagraph applies where:

- the defendant (Person A) makes a threat to Person B and the threat is that serious harm will be caused to Person B, or
- the defendant (Person A) makes a threat to Person B and the threat is that serious harm will be caused to Person C.

998. It is necessary to cover both of these scenarios because foreign interference activities, particularly those undertaken on behalf of foreign governments, often involve interference with the rights of diaspora communities in Australia. For example, a person acting on behalf of Country X might seek to influence the activities of Person Y (a prominent leader of a diaspora community in Australia) by threatening that serious harm will be caused to Person Y's family members who are still living in Country X if Person Y's activities in Australia do not comply with Country X's wishes.

999. Subparagraph 92.3(1)(d)(iii) refers a person making a demand with menaces. Consistent with the definition in section 92.1, the term has the same meaning as in Part 7.5 of the Criminal Code. ***Menaces*** is defined in section 138.2 of the Criminal Code as including a threat (as defined in the Dictionary to the Criminal Code), whether express or implied, of conduct that is detrimental or unpleasant to another person, or a general threat of detrimental or unpleasant conduct that is implied because of the status, office or position of the maker of the threat. A threat against an individual is taken not the be menaces unless:

- the threat would be likely to cause the individual to act unwillingly and the maker of the threat is aware of the vulnerability of the individual to the threat, or
- the threat would be likely to cause a person of normal stability and courage to act unwillingly.

1000. Under subsection 138.2(3), a threat against a person who is not an individual is taken not to be menaces unless the threat would ordinarily cause an unwilling response, or the

threat would be likely to cause an unwilling response because of a particular vulnerability of which the maker of the threat is aware.

1001. Subparagraph 92.3(1)(d)(iii) is intended to capture threats that would generally be considered to be blackmail, rather than the threats to cause serious physical or mental harm covered by subparagraph 92.3(1)(d)(ii). For subparagraph 92.3(1)(d)(iii), the defendant must be the person making the demand with menaces.

1002. Examples of demands with menaces would include:

- a threat to arrest the targeted person upon their entry to another country,
- a threat to bankrupt a business associated with a targeted person, or
- a threat to ensure the targeted person (or one of their family members) is denied a visa for entry to another country.

1003. In the example above, Person E would be aware of a substantial risk that their conduct involved making a threat to cause serious harm and, given the circumstances known to Person E, it is unjustifiable to take that risk.

1004. The maximum penalty for the offence in subsection 92.3(1) is 15 years imprisonment. The commission of this offence would have serious consequences for the sovereignty of Australia. It is unacceptable for foreign principals to seek to influence or intimidate Australians or Australian governments, or pursue their intelligence activities, in a manner that is covert or deceptive or involves threats to cause serious harm or demands with menaces. In the worst case scenario, Australians could be threatened with death by a person acting on behalf of a foreign principal who is aware of a substantial risk that their conduct will prejudice Australia's national security. This justifies the maximum penalty for the offence.

Interference involving targeted person

1005. Subsection 92.3(2) will make it an offence to engage in conduct on behalf of a foreign principal reckless as to whether their conduct will influence another person (the target) in relation to a political or governmental process or the exercise of an Australian democratic or political right without disclosing to the target that they are working for a foreign principal.

1006. This offence will be punishable by a maximum penalty of 15 years imprisonment.

1007. An example of this offence is as follows. Person G is a director of Company H. Although Company H purports to be a private company, in fact its activities are directed and supervised by the government of Country I, which in turn uses the company as a front for its activities. Using Company H's business activities as a justification, Person G builds connections with several members of the Federal parliament and then seeks to convince them to vote in favour of imposing trade sanctions on Country J, a military rival of Country I. Person G presents himself as representing the views of Company H and does not disclose the relationship to Country I to the members of parliament.

1008. To establish this offence, the prosecution will need to prove beyond a reasonable doubt that:

- a person intentionally engaged in conduct

- the:
    - person engaged in the conduct on behalf of a foreign principal
    - person engaged in the conduct on behalf of a person acting on behalf of a foreign principal
    - person engaged in the conduct in collaboration with a foreign principal
    - person engaged in the conduct in collaboration with a person acting on behalf of a foreign principal
    - conduct was directed, funded or supervised by a foreign principal, or
    - conduct was directed, funded or supervised by a person acting on behalf of a foreign principal

  and the person is reckless as to this element.
- the person was reckless as to whether the conduct would influence another person (the target):
    - in relation to a political or governmental process of the Commonwealth or a State or Territory, or
    - in the target's exercise, whether or not in Australia, of an Australian democratic or political right, and
- the person intentionally conceals from, or fails to disclose to, the target the fact that their conduct was:
    - on behalf of a foreign principal
    - on behalf of a person acting on behalf of a foreign principal
    - in collaboration with a foreign principal
    - in collaboration with a person acting on behalf of a foreign principal
    - directed, funded or supervised by a foreign principal, or
    - directed, funded or supervised by a person acting on behalf of a foreign principal.

1009. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 92.3(2)(a) and (d). Under subsection 5.2(1) of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

1010. Recklessness is the fault element for paragraphs 92.3(2)(b) and (c). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and

- a result if he or she is 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 the risk.

1011. For paragraph 92.3(2)(a) of the offence, the prosecution will have to prove beyond a reasonable doubt that the defendant intended to engage in the relevant conduct. Consistent with subsection 4.1(2) of the Criminal Code, the reference to 'engages in conduct' in paragraph 92.3(2)(a) means to do an act or to omit to perform an act.

1012. For paragraph 92.3(2)(b), the prosecution will have to prove beyond a reasonable doubt that the defendant's conduct was engaged in on behalf of, or in collaboration with, a foreign principal, on behalf of a person acting on behalf of a foreign principal, directed, funded or supervised by a foreign principal or a person acting on behalf of a foreign principal. Recklessness is the fault element for this element. Therefore, the defendant must have been aware of a substantial risk that his or her conduct was engaged in on behalf of, or in collaboration with, a foreign principal, on behalf of a person acting on behalf of a foreign principal, directed, funded or supervised by a foreign principal or a person acting on behalf of a foreign principal and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk.

1013. It is possible that a defendant will know, or be reckless, as to the fact that they are engaging in conduct a foreign government because they are being tasked by a person who identifies himself or herself as an official of a foreign government. In this case, the person will be engaging in the conduct on behalf of the foreign principal.

1014. However, it may also be the case that the defendant is not tasked directly by a foreign government official, but by an intermediary. In this case, the prosecution will have to prove beyond a reasonable doubt that the defendant was aware of a substantial risk that he or she was being tasked by a person acting on behalf of a foreign principal and that it was unjustifiable to take that risk. This may be the case where, for example, the intermediary advises the defendant that the intermediary acts in coordination with or provides advice to foreign officials, or the intermediary facilitates preferential treatment for the defendant from a foreign government.

1015. Consistent with subsection 92.3(3), for the purposes of paragraph 92.3(2)(b), the person will not need to have in mind a particular foreign principal and may have in mind more than one foreign principal. For example, a defendant may assist an individual who has identified themselves to the defendant as a foreign official, but has not specified which foreign country they represent. Or, a defendant may provide assistance in the knowledge this assistance will or could assist multiple foreign principals at the same time.

1016. For the purposes of paragraph 92.3(2)(c), the prosecution will have to prove beyond a reasonable doubt that the person was reckless as to whether their act or omission would influence another person (the target):

- in relation to a political or governmental process of the Commonwealth or a State or Territory (subparagraph 92.3(2)(c)(i)), or

- in the target's exercise, whether or not in Australia, of an Australian democratic or political right (subparagraph 92.3(1)(c)(ii)).

1017. Subparagraph 92.3(2)(c)(i) refers to a political or governmental process of the Commonwealth or a State or Territory. The reference to political processes is intended to cover matters within political parties (such as which candidate is pre-selected or the manner in which preferences are to be allocated at an election) as well as political matters within the parliamentary process (such as decisions by shadow Cabinet or decisions by political parties about policies). The reference to governmental processes is intended to cover decision making by the Executive Government, including Cabinet decisions, Executive Council decisions and decisions of individual ministers or departments. The term is intended to cover parliamentary processes such as votes on legislation and establishment and conduct of committees or inquiries.

1018. Subparagraph 92.3(2)(c)(ii) refers to the exercise, whether or not in Australia, of Australian democratic or political rights. This term is intended to cover a broad range of rights held by Australians in relation to participation in Australia's democracy, including voting in elections and referenda and participating in lawful protests. The reference to 'whether or not in Australia' is intended to reflect the fact that Australia's can exercise Australian democratic rights from outside Australia. For example, this element is intended to be sufficiently broad to cover an Australian's right to vote in an Australian election while he or she is physically located outside Australia. The reference to 'Australian' democratic and political rights is intended to limit the operation of this paragraph only to rights that arise because of a person's status as Australian. For example, it is not intended to cover a situation where a person is a joint citizen of Australia and the United Kingdom and has a right to vote in United Kingdom elections while physically located in Australia. This would be a United Kingdom democratic right, rather than an Australian democratic right, even though it is being exercised 'in' Australia.

1019. The offence is targeting undisclosed influence on another person in relation to one of the matters covered by subparagraphs 92.3(2)(c)(i) and (ii). Paragraph 92.3(2)(c) requires the defendant's to be reckless as to whether their conduct would influence another person (known as the target). For example, the defendant may, under direction from a foreign country, seek to influence a Commonwealth Member of Parliament in relation to a pending vote in the House of Representatives. Another example would be where the defendant seeks to influence an Australian citizen as to how they should vote in a Federal election.

1020. In the example above, Person G would be aware of a significant risk that their conduct was influencing another person in relation a political or governmental process, being a vote in Federal Parliament.

1021. For the purposes of paragraph 92.3(2)(d), the prosecution will have to prove beyond a reasonable doubt that the defendant intentionally concealed from, or failed to disclose to, the target the fact that his or her conduct was engaged in on behalf of a foreign principal and that, having regard to the circumstances known to him or her, it is unjustifiable to take that risk.

1022. In the example above, Person G has disclosed their affiliation with Company H but has not disclosed that their conduct was undertaken on behalf of, or at the direction of, Country H.

1023. The maximum penalty for the offence in subsection 92.3(2) is 15 years imprisonment. The commission of this offence would have serious consequences for the sovereignty of Australia. It is unacceptable for foreign principals to seek to influence Australians or Australian governments in relation to political or government processes or the exercise of Australian democratic or political rights. In the worst case scenario, a person could have engaged in conduct in relation to a decision of the Australian Government, aware of a substantial risk that it would influence that decision, without disclosing that the influence is being brought to bear on behalf of a foreign principal. This justifies the maximum penalty for the offence.

Section 92.4 – Offence of preparing for a foreign interference offence

1024. Section 92.4 will establish the offence of preparing for a foreign interference offence. The offence will criminalise conduct in preparation for, or planning, an offence of foreign interference. The offence will be punishable by a maximum penalty of 10 years imprisonment.

1025. An example of this offence is as follows. Person A is an Australian citizen who is tasked with influencing Australian Government policy on Country B. Person A sets up encrypted communications channels with Country B, received detailed tasking about the outcome to be achieved and sets up meetings with several Australian Government ministers.

1026. The purpose of this offence is to give law enforcement means to deal with preparatory conduct and enable intervention before foreign interference occurs.

1027. To establish this offence, the prosecution will need to prove beyond reasonable doubt that:

- the person intentionally engages in conduct, and
- the person does so with the intention of preparing for, or planning, an offence against another provision in Subdivision A (foreign interference).

1028. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 92.4(1)(a). Under section 5.2(1) of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

1029. For paragraph 92.4(1)(a), the prosecution will have to prove beyond a reasonable doubt that the defendant intentionally engaged in the relevant conduct. Consistent with subsection 4.1(2) of the Criminal Code, the reference to 'engages in conduct' in paragraph 92.4(1)(a) means to do an act or to omit to perform an act.

1030. For paragraph 92.4(1)(b), the prosecution will have to prove beyond a reasonable doubt that the person engaged in the conduct with the intention of preparing for, or planning, an offence against another provision in Subdivision A (foreign interference).

1031. The terms preparing and planning are not defined and are intended to take their ordinary meanings.

- The term 'preparing' could include acts to conceive, formulate, make ready, arrange, and assemble an idea, plan, thing, or person for an offence against another provision in Subdivision A (foreign interference).

- The term 'planning' could include acts to organise, arrange, design, draft, or setup an idea, plan, thing, or person for an offence against another provision in Subdivision A (foreign interference).

1032. Given the offences are directed at behaviour at the planning, or planning, stage, it is appropriate to impose the fault element of intention on both of the elements of the offence. This will ensure that a person will only be guilty of this offence where there is sufficient evidence that the person intended to prepare for, or plan, a foreign interference offence.

1033. The maximum penalty for this offence is 10 years imprisonment. While persons who attempt to commit offences are generally subject to the same penalty as if the actual offence had been carried out, the offence at subsection 92.4(1) is intended to capture behaviour at the planning stage, rather than the more advanced stage at which an ancillary offence of attempt could otherwise apply.

1034. Subsection 92.4(2) specifies that section 11.1 (attempt) does not apply to an offence against subsection 92.4(1). Section 11.1 of the Criminal Code extends criminal responsibility for all Commonwealth offences and operates to automatically provide for ancillary offences such as attempting to commit an offence or inciting the commission of an offence. Subsection 92.4(2) modifies the automatic application of section 11.1 in relation to the ancillary offence of attempt. This is appropriate because the offence is already directed at conduct that is preparatory in nature.

1035. Under paragraph 92.4(3)(a), the preparatory offence at subsection 92.4(1) will apply whether or not an offence against Subdivision B is actually committed. This is consistent with the intention behind the offence to allow intervention by law enforcement prior to foreign interference occurring.

1036. Under paragraph 92.4(3)(b), the preparatory offence at subsection 92.4(1) will apply whether or not the person engages in conduct in preparation for, or planning, a specific offence against a provision of Subdivision B. This clarifies that it is not necessary for the prosecution to identify a specific offence – it will be sufficient for the prosecution to prove that the particular conduct was related to 'an' offence. This ensures that the offence will be available where a person has planned a range of activities preparatory to committing a foreign interference offence that are still in the formative stages. For example, where a person has not necessarily decided on a particular target, time or date or other specific details that would constitute one of the specified offences against Subdivision B.

1037. Under paragraph 92.4(3)(c), the preparatory offence at subsection 92.4(1) will apply whether or not the act is done in preparation for, or planning, more than one offence against a provision of Subdivision B. This clarifies that the offence will still apply where a person has engaged in preparatory conduct in relation to several offences against Subdivision B.

Section 92.5 - Defence

1038. The general defences available under Part 2.3 of the Criminal Code will be available to a person accused of an offence under Subdivision B of Division 92. In addition, section 92.5 creates specific defences.

1039. Section 92.5 provides a defence if a person dealt with the relevant information or article:

- in accordance with a law of the Commonwealth (paragraph 92.5(a)), or
- in accordance with an arrangement or agreement to which the Commonwealth is party (paragraph 92.5(b), or
- in the person's capacity as a public official (paragraph 92.5(c)).

1040. It is appropriate for these matters relating to lawful authority to be cast as defences 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.

1041. Consistent with section 13.3 of the Criminal Code, in the case of an evidential burden, the defendant bears the burden of adducing or pointing to evidence that suggests a reasonable possibility that the matter exists or does not exist. If the defendant discharges an evidential burden, the prosecution must disprove those matters beyond reasonable doubt, consistent with section 13.1 of the Criminal Code.

1042. Section 10.5 of the Criminal Code provides a general defence of lawful authority applicable to all Commonwealth offences. This defence is narrow and only applies to conduct that is specifically justified or excused by a law. Consistent with the definition of ***law*** in the Dictionary to the Criminal Code, this means the conduct must be specifically justified or excused by a law of the Commonwealth, and includes the Criminal Code.

1043. The defence at paragraph 92.5(a) is broader than the lawful authority defence available under section 10.5 and will cover a person acting 'in accordance' with a law of the Commonwealth, rather than the law of the Commonwealth needing to specifically justify or excuse the person's conduct.

1044. The defence at paragraph 92.5(b) applies when person dealt with the information or article in accordance with an agreement or arrangement to which the Commonwealth is party. This defence provides that the foreign interference offences in Subdivision B do not apply if a person's conduct was in accordance with an agreement or arrangement to which the Commonwealth was a party.

1045. The terms 'arrangement' and 'agreement' are not defined and will be given their ordinary meaning. The term 'agreement' is not intended to be limited by the meaning of 'agreement' in Australian international practice as being a treaty, nor is it intended to require evidence of a formal contractual or legal agreement. It is intended that such terms will capture agreements or arrangements in a range of forms, including those made by exchange of letters or as a memorandum of understanding.

1046. The defence at paragraph 92.5(c) applies when a person dealt with the information or article in the person's capacity as a public official. ***Public official*** is defined in the Dictionary to the Criminal Code to include:

- a Commonwealth public official
- an officer or employee of the Commonwealth or of a State or Territory
- an individual who performs work for the Commonwealth, or for a State or Territory, under a contract
- an individual who holds or performs the duties of an office established by a law of the Commonwealth or of a State or Territory
- an individual who is otherwise in the service of the Commonwealth or of a State or Territory (including service as a member of a military force or police force)
- a member of the executive, judiciary or magistracy of the Commonwealth or of a State or Territory, and
- an officer or employee of:
    - an authority of the Commonwealth, or
    - an authority of a State or Territory.

1047. ***Commonwealth public official*** is defined in the Dictionary to the Criminal Code to mean:

- the Governor-General
- a person appointed to administer the Government of the Commonwealth under section 4 of the Constitution
- a Parliamentary Secretary
- a member of either House of the Parliament
- an individual who holds an appointment under section 67 of the Constitution
- the Administrator, an Acting Administrator, or a Deputy Administrator, of the Northern Territory
- a Commonwealth judicial officer (as defined in the Dictionary to the Criminal Code)
- an APS employee
- an individual employed by the Commonwealth other than under the *Public Service Act 1999*

- a member of the Australian Defence Force
- a member or special member of the AFP
- an individual (other than an official of a registered industrial organisation) who holds or performs the duties of an office established by or under a law of the Commonwealth, other than:
    - the *Corporations (Aboriginal and Torres Strait Islander) Act 2006*
    - the *Australian Capital Territory (Self-Government) Act 1988*
    - the *Corporations Act 2001*
    - the *Norfolk Island Act 1979*, or
    - the *Northern Territory (Self-Government) Act 1978*
- an officer or employee of a Commonwealth authority
- an individual who is a contracted service provider for a Commonwealth contract
- an individual who is an officer or employee of a contracted service provider for a Commonwealth contract and who provides services for the purposes (whether direct or indirect) of the Commonwealth contract
- an individual (other than an official of a registered industrial organisation) who exercises powers, or performs functions, conferred on the person by or under a law of the Commonwealth, other than:
    - the *Corporations (Aboriginal and Torres Strait Islander) Act 2006*
    - the *Australian Capital Territory (Self-Government) Act 1988*
    - the *Corporations Act 2001*
    - the *Norfolk Island Act 1979*
    - the *Northern Territory (Self-Government) Act 1978*, or
    - a provision specified in the regulations
- an individual who exercises powers, or performs functions, conferred on the person under a law in force in the Territory of Christmas Island or the Territory of Cocos (Keeling) Islands (whether the law is a law of the Commonwealth or a law of the Territory concerned), or
- the Registrar, or a Deputy Registrar, of Aboriginal and Torres Strait Islander Corporations.

1048. This defence is intended to apply where a person engages in conduct covered by the foreign interference offences in the person's capacity as a public official. This may include, for example, an employee duty statement, a policy guidance document or employee practice manual, or previous examples of the same conduct which has been authorised by superiors.

1049. Many departments and agencies engage in joint activities with international counterparts as part of their normal business dealings. The offences in Subdivision B are only intended to apply where a person's conduct is not a proper or legitimate part of their work. It will not be a defence to a charge of foreign interference where a person has gone beyond their ordinary duties.

1050. Note 1 under the defence at section 92.5 clarifies that the defendant will bear an evidentiary burden in relation to this defence. Consistent with section 13.3 of the Criminal Code, the defendant will need to point to evidence that suggests a reasonable possibility that the defence is made out. If this is done, the prosecution must refute the defence beyond reasonable doubt (section 13.1).

1051. Both AFP and CDPP consider the availability of any defences when considering whether to investigate and prosecute criminal offences. In relation to prosecution decisions, the Prosecution Policy of the Commonwealth specifically requires the CDPP to take into account any lines of defence which are plainly open to, or have been indicated by, the alleged offender in deciding whether there is a reasonable prospect of a conviction being secured. Subsection 93.1 (to be inserted by Item 18 of Schedule 1) requires the Attorney-General consider whether the defendant's conduct is authorised under the defences in section 92.5 before providing his or her consent to the institution of proceedings for the commitment of a person for trial for an offence to which the defence applies.

Section 92.6 – Geographical jurisdiction

1052. Section 92.6 applies Section 15.2 of the Criminal Code (extended geographical jurisdiction – Category B) to Subdivision B of Division 92.

1053. Under section 15.2, the effect of Category B jurisdiction is that the offence applies:

- if the conduct constituting the offence occurs wholly or partly in Australia
- if the result of that conduct occurs wholly or partly in Australia, and
- if the conduct occurs outside Australia and at the time of committing the offence, the person is an Australian citizen, resident or body corporate.

1054. Category B jurisdiction is appropriate to ensure that this offence appropriately protects Australia's from foreign interference that occurs in Australia or where the result occurs in Australia. The application of Category B jurisdiction also prevents Australian citizens, residents or bodies corporate from engaging in foreign interference offences, wherever that conduct occurs.

Subdivision C – Foreign interference involving foreign intelligence agencies

Section 92.7 – Knowingly supporting foreign intelligence agency

1055. Section 92.7 makes it an offence to provide support or resources to an organisation or a person acting on behalf on an organisation where the person knows that the organisation is a foreign intelligence organisation. This offence will be punishable by a maximum of 15 years imprisonment.

1056. An example of this offence is as follows. Person A is an Australian citizen with an ongoing relationship with Person B, whom Person A knows is a foreign intelligence service officer. In response to specific requests from Person B, Person A makes a series of administrative arrangements that will facilitate Person B's movements and activities within Australia. Person A believes that Person B is travelling to Australia for operational purposes but is unaware of the specific activity Person B is conducting.

1057. To establish this offence, the prosecution will have to prove beyond reasonable doubt that:

- a person intentionally provides support or resources to an organisation or a person acting on behalf of an organisation, and
- the organisation is a foreign intelligence agency and the person knows this.

1058. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 92.7(a). Under subsection 5.2(1) of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

1059. Paragraph 92.7(b) specifies that a fault element of knowledge applies. Under section 5.3 of the Criminal Code, a person has knowledge of a circumstance if he or she is aware that it exists or will exist in the ordinary course of events.

1060. For paragraph 92.7(a), the prosecution must prove beyond reasonable doubt that the defendant intended to provide support or resources to an organisation, or a person acting on behalf of the organisation.

1061. The terms 'support' and 'resources' are not defined and will be given their ordinary meaning. What constitutes providing support or resources to an organisation will depend on the facts of each case but it is intended to cover 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 organisations activities, operations, or objectives.

1062. In the example above, Person A has provided support and resources to Person B by subscribing multiple telephones and booking a hotel room for Person B to use while in Australia.

1063. For paragraph 92.7(b), the prosecution will have to prove that the organisation to which the person provides support or resources is a foreign intelligence agency. The person will have to know that the organisation is a foreign intelligence agency.

1064. The definition of ***foreign intelligence agency*** in the Dictionary to the Criminal Code, to be inserted by Item 24 of Schedule 1, means an intelligence or security service (however

described) of a foreign country. The term ***foreign country*** is defined in the Dictionary to the Criminal Code as including a colony or overseas territory, and a territory outside Australia, where a foreign country is to any extent responsible for the international relations of the territory, and a territory outside Australia this is to some extent self-governing, but that is not recognised as an independent sovereign state by Australia.

1065. The definition of 'foreign intelligence agency' is intentionally broad to capture the range of intelligence agencies that exist in various countries. Such agencies will generally, but not always, have comparable functions to agencies in the Australian Intelligence Community, as set out at the definition of ***domestic intelligence agency*** in section 121.1 of Schedule 2 of this Bill. This includes:

- the Australian Secret Intelligence Service
- ASIO
- the Australian Geospatial-Intelligence Organisation
- the Defence Intelligence Organisation
- the Australian Signals Directorate, and
- the Office of National Assessments.

1066. To prove knowledge on the part of the defendant, the prosecution will have to demonstrate either that the defendant knew the organisation engaged in intelligence activities on behalf of a foreign country, or, if the organisation is a declared or publicly acknowledged foreign intelligence organisation, that the defendant knew this fact.

1067. In the example above, Person A is aware that Person B is acting on behalf of a foreign intelligence service, which clearly meets the definition of foreign intelligence agency in the Dictionary. Therefore, Person A knows that the organisation to which he or she is providing support and resources is a foreign intelligence agency.

1068. The note to section 92.7 specifies that an alternative verdict may be available for an offence against section 92.7 in accordance with section 93.5.

1069. 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.

<u>Section 92.8 – Recklessly supporting foreign intelligence agency</u>

1070. Section 92.8 makes it an offence to provide support or resources to an organisation or a person acting on behalf on an organisation where the person knows that the organisation is

a foreign intelligence organisation. This offence will be punishable by a maximum of 10 years imprisonment.

1071. An example of this offence is as follows. Person A is an Australian citizen with an ongoing relationship with Person B. Person A knows that Person B is employed by a foreign government, but does not know the specific agency. Person B insists that Person A follow specific communication methods whenever contacting Person B, and Person A is aware that Person B uses several different names. In response to specific requests from Person B, Person A attends dissident group meetings in Australia and provides a list of attendees to Person B. Person A also uses open source materials to find identifying details for several of the attendees, which Person A passes to Person B.

1072. To establish this offence, the prosecution will have to prove beyond reasonable doubt that:

- a person intentionally provides support or resources to an organisation or a person acting on behalf of an organisation, and
- the organisation is a foreign intelligence agency and the person was reckless as to this element.

1073. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 92.8(a). Under subsection 5.2(1) of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

1074. Recklessness is the fault element for paragraph 92.8(b). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and
- a result if he or she is 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 the risk.

1075. For paragraph 92.8(a), the prosecution must prove beyond reasonable doubt that the defendant intended to provide support or resources to an organisation, or a person acting on behalf of the organisation.

1076. The terms ‘support’ and ‘resources’ are not defined and will be given their ordinary meaning. What constitutes providing support or resources to an organisation will depend on the facts of each case but it is intended to cover 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 organisations activities, operations, or objectives.

1077. In the example above, Person A has provided support and resources to Person B by compiling a list of attendees at dissident group meetings and providing their addresses and phone numbers.

1078. For paragraph 92.8(b), the prosecution will have to prove that the organisation to which they provide support or resources is a foreign intelligence agency. Recklessness is the fault element for this element. Therefore, the person will need to be aware of a substantial risk that the organisation is a foreign intelligence agency and, having regard to the circumstances known to the person, it is unjustifiable to take the risk.

1079. The definition of ***foreign intelligence agency*** in the Dictionary to the Criminal Code, to be inserted by Item 24 of Schedule 1, means an intelligence or security service (however described) of a foreign country. The term ***foreign country*** is defined in the Dictionary to the Criminal Code as including a colony or overseas territory, and a territory outside Australia, where a foreign country is to any extent responsible for the international relations of the territory, and a territory outside Australia this is to some extent self-governing, but that is not recognised as an independent sovereign state by Australia.

1080. The definition of 'foreign intelligence agency' is intentionally broad to capture the range of intelligence agencies that exist in various countries. Such agencies will generally, but not always, have comparable functions to agencies in the Australian Intelligence Community, as set out at the definition of ***domestic intelligence agency*** in section 121.1 of Schedule 2 of this Bill. This includes:

- the Australian Secret Intelligence Service
- ASIO
- the Australian Geospatial-Intelligence Organisation
- the Defence Intelligence Organisation
- the Australian Signals Directorate, and
- the Office of National Assessments.

1081. In the example above, Person A is aware that Person B is employed by a foreign government, uses several different identities and insists on using encrypted communications. Therefore, Person A would be aware of a substantial risk that Person B is a person acting on behalf of a foreign intelligence agency.

1082. The maximum penalty of 10 years imprisonment is less than the more serious offence of knowingly supporting a foreign intelligence agency at section 92.7. A penalty of 10 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.

<u>Section 92.9 – Knowingly funding or being funded by foreign intelligence agency</u>

1083. Section 92.9 will make it an offence for a person to fund or be funded by a foreign intelligence agency. The offence will apply where a person receives or obtains funds from, make funds available to, or collects funds for or on behalf of, a foreign intelligence agency. The offence will only apply where the person knows that the organisation is a foreign intelligence agency. This offence will be punishable by a maximum of 15 years imprisonment.

1084. An example of this offence is as follows. Person A is an Australian citizen, and maintains an information technology business that is used to support the activities of foreign nationals Person A knows to be foreign intelligence officers of Country X. These officers of Country X transfer substantial funds to Person A to support the business, on the understanding the business is kept viable for future use in Country X's intelligence activities.

1085. To establish this offence, the prosecution will have to prove beyond reasonable doubt that:

- a person intentionally (either directly or indirectly):
    - receives or obtains funds from an organisation
    - receives or obtains funds from a person acting on behalf of an organisation
    - makes funds available to an organisation
    - makes funds available to a person acting on behalf of an organisation
    - collects funds for or on behalf of an organisation, or
    - collects funds for or on behalf a person acting on behalf of an organisation, and
- the organisation is a foreign intelligence agency and the person knows this.

1086. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to subparagraphs 92.9(a)(i) and (ii). Under subsection 5.2(1) of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

1087. Paragraph 92.9(b) specifies that the fault element for this element is knowledge. Under section 5.3 of the Criminal Code, a person has knowledge of a circumstance if he or she is aware that it exists or will exist in the ordinary course of events.

1088. For paragraph 92.9(a), the prosecution must prove beyond reasonable doubt that the defendant intentionally receives or obtain funds from, make funds available to, or collect fund for or on behalf of, an organisation or a person acting on behalf of an organisation. This can occur either directly or indirectly.

1089. The term 'funds' is not defined and will take it ordinary meaning. It is intended that the term will be construed broadly and would cover financing through money, loans, agreements, appropriations, contracts, or promises of funding, in whole or in part.

1090. Subparagraph 92.9(a)(i) applies where a person receives or obtains funds from an organisation or a person is acting on behalf of the organisation, or where a person makes funds available to an organisation or a person acting on behalf of an organisation. A person 'receives' or 'obtains' funds where the person is given, provided or otherwise acquires the funds from the organisation. A person makes funds available when they give or provide the funds to the organisation by whatever means available. This includes where a person provides or loans money to an organisation on the understanding that the money will later be returned or paid back.

1091. In the example above, Person A has made funds directly available to a person acting on behalf of an organisation by providing money to an employee of the intelligence services of Country X. Person A has also received funds from the intelligence services in Country X. This has occurred indirectly in the form of a loan form company Y.

1092. Subparagraph 92.9(a)(ii) applies where a person collects funds for on behalf of an organisation or a person acting on behalf of an organisation. The phrase 'on behalf of' is intended to include where a person or entity represents, acts in the interests of, or acts as a proxy for, the organisation. For example, a person may act as an intermediary for a foreign intelligence service in Australia and be instructed to collect funds from a specific person or location and then provide the funds to an employee of the foreign intelligence service. In this case the person would be collecting funds on behalf of an organisation.

1093. For paragraph 92.9(b), the prosecution will have to prove that the organisation to which the person provides support or resources is a foreign intelligence agency. The person must know that the organisation is a foreign intelligence agency.

1094. The definition of ***foreign intelligence agency*** in the Dictionary to the Criminal Code, to be inserted by Item 24 of Schedule 1, means an intelligence or security service (however described) of a foreign country. The term ***foreign country*** is defined in the Dictionary to the Criminal Code as including a colony or overseas territory, and a territory outside Australia, where a foreign country is to any extent responsible for the international relations of the territory, and a territory outside Australia this is to some extent self-governing, but that is not recognised as an independent sovereign state by Australia.

1095. The definition of 'foreign intelligence agency' is intentionally broad to capture the range of intelligence agencies that exist in various countries. Such agencies will generally, but not always, have comparable functions to agencies within the Australian Intelligence Community, as set out at the definition of ***domestic intelligence agency*** in section 121.1 of Schedule 2 of this Bill. This includes:

- the Australian Secret Intelligence Service
- ASIO
- the Australian Geospatial-Intelligence Organisation
- the Defence Intelligence Organisation
- the Australian Signals Directorate, and
- the Office of National Assessments.

1096. To prove knowledge on the part of the defendant, the prosecution will have to demonstrate either that the defendant knew the organisation engaged in intelligence activities on behalf of a foreign country, or, if the organisation is a declared or publically acknowledged foreign intelligence organisation, that the defendant knew this fact.

1097. The note to section 92.9 specifies that an alternative verdict may be available for an offence against section 92.9 in accordance with section 93.5. Section 93.5 allows for an alternative verdict if the trier of fact is not satisfied that the defendant is guilty of the offence

in section 92.9, but is satisfied of the offence against section 92.10 (i.e. if the trier of fact is not satisfied that the defendant knew the organisation was a foreign intelligence organisation but is satisfied that the defendant was reckless as to whether the organisation is a foreign intelligence organisation).

1098. 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.

Section 92.10 – Recklessly funding or being funded by foreign intelligence agency

1099. Section 92.10 will make it an offence for a person to fund or be funded by a foreign intelligence agency. The offence will apply where a person receives or obtains funds from, make funds available to, or collects funds for or on behalf of, a foreign intelligence agency. The offence will apply where the person is reckless as to whether the organisation is a foreign intelligence agency. This offence will be punishable by a maximum of 10 years imprisonment.

1100. An example of this offence is as follows. Person B is an Australian citizen who undertakes *ad hoc* tasks for foreign individuals employed by the government of Country Y, in return for preferential treatment they facilitate in Country Y. Based on the requests made, Person B suspects these officials are foreign intelligence officers. In response to a specific request from these Country Y officers, Person B attends a prearranged location and gives a large sum of Person B's own money to Person C, a visiting Country Y national Person B has not met before. Person B does not know what the money will be used for.

1101. To establish this offence, the prosecution will have to prove beyond reasonable doubt that:

- a person intentionally (either directly or indirectly):
    - receives or obtains funds from an organisation
    - receives or obtains funds from a person acting on behalf of an organisation
    - makes funds available to an organisation
    - makes funds available to a person acting on behalf of an organisation
    - collects funds for or on behalf of an organisation, or
    - collects funds for or on behalf a person acting on behalf of an organisation, and
- the organisation is a foreign intelligence agency and the person is reckless as to this element.

1102. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to subparagraphs 92.10(a)(i) and (ii). Under subsection 5.2(1) of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

1103. Recklessness is the fault element for paragraph 92.10(b). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and

- a result if he or she is 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 the risk.

1104. For paragraph 92.10(a), the prosecution must prove beyond reasonable doubt that the defendant intentionally receives or obtain funds from, make funds available to, or collect fund for or on behalf of, an organisation or a person acting on behalf of an organisation. This can occur either directly or indirectly.

1105. The term 'funds' is not defined and will take it ordinary meaning. It is intended that the term will be construed broadly and would cover financing through money, loans, agreements, appropriations, contracts, or promises of funding, in whole or in part.

1106. Subparagraph 92.10(a)(i) applies where a person receives or obtains funds from an organisation or a person is acting on behalf of the organisation, or where a person makes funds available to an organisation or a person acting on behalf of an organisation. A person 'receives' or 'obtains' funds where the person is given, provided or otherwise acquires the funds from the organisation. A person makes funds available when they give or provide the funds to the organisation by whatever means available. This includes where a person provides or loans money to an organisation on the understanding that the money will later be returned or paid back.

1107. In the example above, Person C has received funds from, and is in the process of making funds available to a person acting on behalf of an organisation. This has occurred directly in the form Person C collecting and delivering cash.

1108. Subparagraph 92.10(a)(ii) applies where a person collects funds for on behalf of an organisation or a person acting on behalf of an organisation. The phrase 'on behalf of' is intended to include where a person or entity represents, acts in the interests of, or acts as a proxy for, the organisation. For example, a person may act as an intermediary for a foreign intelligence service in Australia and be instructed to collect funds from a specific person or location and then provide the funds to an employee of the foreign intelligence service. In this case the person would be collecting funds on behalf of an organisation.

1109. For paragraph 92.10(b), the prosecution will have to prove that the organisation to which they provide support or resources is a foreign intelligence agency. Recklessness is the fault element for this element. Therefore, the person will need to be aware of a substantial risk that the organisation is a foreign intelligence agency and, having regard to the circumstances known to the person, it is unjustifiable to take the risk.

1110. The definition of ***foreign intelligence agency*** in the Dictionary to the Criminal Code, to be inserted by Item 24 of Schedule 1, means an intelligence or security service (however described) of a foreign country. The term ***foreign country*** is defined in the Dictionary to the Criminal Code as including a colony or overseas territory, and a territory outside Australia, where a foreign country is to any extent responsible for the international relations of the territory, and a territory outside Australia this is to some extent self-governing, but that is not recognised as an independent sovereign state by Australia.

1111. The definition of 'foreign intelligence agency' is intentionally broad to capture the range of intelligence agencies that exist in various countries. Such agencies will generally, but not always, have comparable functions to agencies within the Australian Intelligence Community, as set out at the definition of ***domestic intelligence agency*** in section 121.1 of Schedule 2 of this Bill. This includes:

- the Australian Secret Intelligence Service
- ASIO
- the Australian Geospatial-Intelligence Organisation
- the Defence Intelligence Organisation
- the Australian Signals Directorate, and
- the Office of National Assessments.

1112. In the example above, Person C has received the money from someone who is suspected to be a foreign intelligence official. The arrangements for communication and collection of the money also suggest that the money is being made available to a foreign intelligence agency.

1113. The maximum penalty of 10 years imprisonment is less than the more serious offence of knowingly supporting a foreign intelligence agency at section 92.9. A penalty of 10 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.

<u>Section 92.11 - Defence</u>

1114. The general defences available under Part 2.3 of the Criminal Code will be available to a person accused of an offence against Subdivision C of Division 92. In addition, section 92.11 creates specific defences.

1115. Section 92.11 provides a defence if a person dealt with the relevant information or article:

- in accordance with a law of the Commonwealth (paragraph 92.11(a)), or
- in accordance with an arrangement or agreement to which the Commonwealth is party (paragraph 92.11(b), or

- in the person's capacity as a public official (paragraph 92.11(c)).

1116. It is appropriate for these matters relating to lawful authority to be cast as defences 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.

1117. Consistent with section 13.3 of the Criminal Code, in the case of an evidential burden, the defendant bears the burden of adducing or pointing to evidence that suggests a reasonable possibility that the matter exists or does not exist. If the defendant discharges an evidential burden, the prosecution must disprove those matters beyond reasonable doubt, consistent with section 13.1 of the Criminal Code.

1118. Section 10.5 of the Criminal Code provides a general defence of lawful authority applicable to all Commonwealth offences. This defence is narrow and only applies to conduct that is specifically justified or excused by a law. Consistent with the definition of ***law*** in the Dictionary to the Criminal Code, this means the conduct must be specifically justified or excused by a law of the Commonwealth, and includes the Criminal Code.

1119. The defence at paragraph 92.11(a) is broader than the lawful authority defence available under section 10.5 and will cover a person acting 'in accordance' with a law of the Commonwealth, rather than the law of the Commonwealth needing to specifically justify or excuse the person's conduct.

1120. The defence at paragraph 92.11(b) applies when person dealt with the information or article in accordance with an agreement or arrangement to which the Commonwealth is party. This defence provides that the foreign interference offences in Subdivision C do not apply if a person's conduct was in accordance with an agreement or arrangement to which the Commonwealth was a party.

1121. The terms 'arrangement' and 'agreement' are not defined and will be given their ordinary meaning. The term "agreement" is not intended to be limited by the meaning of 'agreement' in Australian international practice as being a treaty, nor is it intended to require evidence of a formal contractual or legal agreement. It is intended that such terms will capture agreements or arrangements in a range of forms, including those made by exchange of letters or as a memorandum of understanding.

1122. The defence at paragraph 92.11(c) applies when a person dealt with the information or article in the person's capacity as a public official. ***Public official*** is defined in the Dictionary to the Criminal Code to include:

- a Commonwealth public official
- an officer or employee of the Commonwealth or of a State or Territory
- an individual who performs work for the Commonwealth, or for a State or Territory, under a contract
- an individual who holds or performs the duties of an office established by a law of the Commonwealth or of a State or Territory

- an individual who is otherwise in the service of the Commonwealth or of a State or Territory (including service as a member of a military force or police force)
- a member of the executive, judiciary or magistracy of the Commonwealth or of a State or Territory, and
- an officer or employee of:
    - an authority of the Commonwealth, or
    - an authority of a State or Territory.

1123. ***Commonwealth public official*** is defined in the Dictionary to the Criminal Code to mean:

- the Governor-General
- a person appointed to administer the Government of the Commonwealth under section 4 of the Constitution
- a Parliamentary Secretary
- a member of either House of the Parliament
- an individual who holds an appointment under section 67 of the Constitution
- the Administrator, an Acting Administrator, or a Deputy Administrator, of the Northern Territory
- a Commonwealth judicial officer (as defined in the Dictionary to the Criminal Code)
- an APS employee
- an individual employed by the Commonwealth other than under the *Public Service Act 1999*
- a member of the Australian Defence Force
- a member or special member of the AFP
- an individual (other than an official of a registered industrial organisation) who holds or performs the duties of an office established by or under a law of the Commonwealth, other than:
    - the *Corporations (Aboriginal and Torres Strait Islander) Act 2006*
    - the *Australian Capital Territory (Self-Government) Act 1988*
    - the *Corporations Act 2001*

    - the *Norfolk Island Act 1979*, or
    - the *Northern Territory (Self-Government) Act 1978*
- an officer or employee of a Commonwealth authority
- an individual who is a contracted service provider for a Commonwealth contract
- an individual who is an officer or employee of a contracted service provider for a Commonwealth contract and who provides services for the purposes (whether direct or indirect) of the Commonwealth contract
- an individual (other than an official of a registered industrial organisation) who exercises powers, or performs functions, conferred on the person by or under a law of the Commonwealth, other than:
    - the *Corporations (Aboriginal and Torres Strait Islander) Act 2006*
    - the *Australian Capital Territory (Self-Government) Act 1988*
    - the *Corporations Act 2001*
    - the *Norfolk Island Act 1979*
    - the *Northern Territory (Self-Government) Act 1978*, or
    - a provision specified in the regulations
- an individual who exercises powers, or performs functions, conferred on the person under a law in force in the Territory of Christmas Island or the Territory of Cocos (Keeling) Islands (whether the law is a law of the Commonwealth or a law of the Territory concerned), or
- the Registrar, or a Deputy Registrar, of Aboriginal and Torres Strait Islander Corporations.

1124. This defence is intended to apply where a person engages in conduct covered by the foreign interference offences in the person's capacity as a public official. This may include, for example, an employee duty statement, a policy guidance document or employee practice manual, or previous examples of the same conduct which has been authorised by superiors.

1125. Many departments and agencies provide support to the foreign intelligence agencies of allies as part of their normal business dealings. The offences in Subdivision C are only intended to apply where a person's conduct is not a proper or legitimate part of their work. It will not be a defence to a charge of foreign interference where a person has gone beyond their ordinary duties.

1126. Note 1 under the defence at subsection 92.11 clarifies that the defendant will bear an evidentiary burden in relation to this defence. Consistent with section 13.3 of the Criminal Code, the defendant will need to point to evidence that suggests a reasonable possibility that

the defence is made out. If this is done, the prosecution must refute the defence beyond reasonable doubt (section 13.1).

1127. Both AFP and CDPP consider the availability of any defences when considering whether to investigate and prosecute criminal offences. In relation to prosecution decisions, the Prosecution Policy of the Commonwealth specifically requires the CDPP to take into account any lines of defence which are plainly open to, or have been indicated by, the alleged offender in deciding whether there is a reasonable prospect of a conviction being secured. Subsection 93.1 (to be inserted by Item 18 of Schedule 1) requires the Attorney-General consider whether the defendant's conduct is authorised under the defences in section 92.11 before providing his or her consent to the institution of proceedings for the commitment of a person for trial for an offence to which the defence applies.

Division 92A – Theft of trade secrets involving foreign principal

Section 92A.1 – Theft of trade secrets involving foreign principal

1128. Section 92A.1 will make it an offence to dishonestly receive, obtain, take, copy or duplicate, sell, buy or disclose information that is a trade secret on behalf of a foreign government principal.

1129. This offence will be punishable by a maximum penalty of 15 years imprisonment.

1130. An example of this offence is as follows. Person A is employed by an Australian company and works with sensitive satellite imaging technology. The technology is only able to be accessed and used by a very limited number of authorised personnel and is not public knowledge. Person A is approached by a representative of the government of Country X, who makes it clear that the technology would be very useful to Country X, and would have a high commercial value if it was provided to them. Person A secretly make copies of information related to the satellite imaging technology. Government X pays Person A a significant amount of money each time he/she provides copies of the sensitive information to them.

1131. To establish this offence, the prosecution will need to prove beyond reasonable doubt that:

- the person intentionally dishonestly receives, obtains, takes, copies or duplicates, sells, buys or discloses information
- all of the following circumstances exist:
    - the information was not generally known in trade or business, or in that particular trade or business concerned
    - the information had an economic value, or a higher economic value that it otherwise would have, because it was not known in trade or business or the trade or business concerned
    - that the owner of the information had made reasonable efforts in the circumstances to prevent that information from becoming generally known, and

and the person is reckless as to these circumstances, and

- the:
    - person engaged in the conduct on behalf of a foreign principal
    - person engaged in the conduct on behalf of a person acting on behalf of a foreign principal
    - person engaged in the conduct in collaboration with a foreign principal
    - person engaged in the conduct in collaboration with a person acting on behalf of a foreign principal
    - conduct was directed, funded or supervised by a foreign principal, or
    - conduct was directed, funded or supervised by a person acting on behalf of a foreign principal

  and the person is reckless as to this element.

1132. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 92A.1(1)(a). Under subsection 5.2(1) of the Criminal Code, a person has the intention with respect to conduct if he or she means to engage in that conduct.

1133. Recklessness is the fault element for paragraphs 92A.1(1)(b) and (c). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and
- a result if he or she is 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 the risk.

1134. For paragraph 92A.1(1)(a), the prosecution must prove beyond reasonable doubt that the defendant intended to dishonestly receive, obtain, take, copy or duplicate, sell, buy or disclose information. ***Information*** is defined in section 90.1 of the Criminal Code to mean information of any kind, whether true or false and whether in a material form or not, and includes an opinion and a report of a conversation.

1135. Consistent with subsection 92A.1(2), for the purposes of paragraph 92A.1(1)(a), ***dishonest*** means:

- dishonest according to the standards of ordinary people, and
- known by the defendant to be dishonest according to the standards of ordinary people.

1136. Subsection 92A.1(3) provides that, in a prosecution for an offence against section 92A(1), the determination of dishonesty is a matter for the trier of fact. Subsections 92A.1(2) and (3) are consistent with other provisions in the Criminal Code relating to dishonesty (see sections 130.3 and 130.4 in Chapter 7 of the Criminal Code).

1137. For the purposes of paragraph 92A.1(1)(b), the prosecution will have to prove beyond a reasonable doubt that the information was information that was not generally known, had a commercial value because it was not known, and that the owner of the information had made reasonable efforts to prevent the information from becoming generally known. Recklessness is the fault element for this element. Therefore the person will have to be aware of a substantial risk that these circumstances exist and that having regard to the circumstances to know him or her, that it was unjustifiable for the defendant to have taken that risk

1138. Although the offence at section 92A.1 does not use the term 'trade secret', the circumstances listed at paragraph 92A.1(1)(b) are intended to cover the types of information that are considered to warrant protection. The circumstances must all apply in order for the offence to be committed. The circumstances listed in paragraph 92A.1(1) are consistent with international examples of definitions of 'trade secrets'. For example, the Canadian *Security of Information Act* defines a 'trade secret' to mean any information, including a formula, pattern, compilation, program, method, technique, process, negotiation position or strategy or any information contained or embodied in a product, device or mechanism that:

- is or may be used in a trade or business
- is not generally known in that trade or business
- has economic value from not being generally known, and
- is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

1139. The United States Code defines a trade secret in 18 USC 1839 to mean all forms and types of financial, business, scientific, technical, economic, or engineering information, whether tangible or intangible and however stored or compiled if:

- the owner thereof has taken reasonable measures to keep such information secret, and
- the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.

1140. For paragraph 92A.1(1)(c), the prosecution will have to prove beyond a reasonable doubt that the defendant's conduct was engaged in on behalf of, or in collaboration with, a foreign principal, on behalf of a person acting on behalf of a foreign principal, directed, funded or supervised by a foreign principal or a person acting on behalf of a foreign principal. Recklessness is the fault element for this element. Therefore, the defendant must have been aware of a substantial risk that his or her conduct was engaged in on behalf of, or in collaboration with, a foreign principal, on behalf of a person acting on behalf of a foreign principal, directed, funded or supervised by a foreign principal or a person acting on behalf of

a foreign principal and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk.

1141. For the purposes of this section ***foreign government principal*** has the same meaning as that given is section 90.3, which provides that each of the following is a ***foreign government principal***:

- the government of a foreign country or a part of a foreign country
- an authority of the government of a foreign country
- an authority of the government of part of a foreign country
- a foreign local government body or foreign regional government body
- a company to which any of the subparagraphs of paragraph (a) of the definition of foreign public enterprise in section 70.1 applies
- a body or association to which either of the subparagraphs of paragraph (b) of the definition of foreign public enterprise in section 70.1 applies
- a foreign political organisation, or
- an entity or organisation directed or controlled:
    - by a foreign government principal within the meaning of any other paragraph of this definition, or
    - by two or more such foreign government principals that are foreign government principals of the same foreign country.

1142. It is possible that a defendant will know, or be reckless, as to the fact that they are engaging in conduct a foreign government because they are being tasked by a person who identifies himself or herself as an official of a foreign government. In this case, the person will be engaging in the conduct on behalf of the foreign principal.

1143. However, it may also be the case that the defendant is not tasked directly by a foreign government official, but by an intermediary. In this case, the prosecution will have to prove beyond a reasonable doubt that the defendant was aware of a substantial risk that he or she was being tasked by a person acting on behalf of a foreign principal and that it was unjustifiable to take that risk. This may be the case where, for example, the intermediary advises the defendant that the intermediary acts in coordination with foreign officials, or the intermediary facilitates preferential treatment for the defendant from a foreign government.

1144. Consistent with subsection 92A.1(4), for the purposes of paragraph 92A.1(1)(c), the person will not need to have in mind a particular foreign principal and may have in mind more than one foreign principal. For example, a defendant may assist an individual who has identified themselves to the defendant as a foreign official, but has not specified which foreign country they represent. Or, a defendant may provide assistance in the knowledge this assistance will or could assist multiple foreign principals at the same time.

1145. The maximum penalty for the offence in subsection 92A.1(1) is 15 years imprisonment. The commission of this offence would have serious consequences for Australia's security and economic interests. It is unacceptable for foreign principals to seek to interfere in Australia's commercial dealings and trade relations. The penalty is consistent with comparable offences in which provide for a link with a foreign principal including section 91.8 (espionage on behalf of a foreign principal) and section 92.3 (offence of reckless foreign interference).

Section 92A.2 – Geographical jurisdiction

1146. Subsection 92A.2(1) applies section 15.2 (extended geographical jurisdiction—Category B) to section 92A.1.

1147. Under section 15.2, the effect of Category B jurisdiction is that the offence applies:

- if the conduct constituting the offence occurs wholly or partly in Australia
- if the result of that conduct occurs wholly or partly in Australia, and
- if the conduct occurs outside Australia and at the time of committing the offence, the person is an Australian citizen, resident or body corporate.

1148. Category B jurisdiction is appropriate to ensure that this offence appropriately protects theft of Australia's trade secrets where the conduct occurs in Australia. The application of Category B jurisdiction also prevents Australian citizens, residents or bodies corporate from engaging in theft of trade secrets on behalf of a foreign government principal, wherever that conduct occurs.

1149. Subsection 92A.2(2) makes clear that subsections 15.2(2) and 15.2(4) (defences for primary and ancillary offences) do not apply to section 92A.2. Both subsections 15.2(2) and 15.2(4) provide a defence for conduct that occurs wholly outside of Australia by an offender who is not an Australian citizen or Australian body corporate, if the foreign country where the offence has taken place does not have in force a law that makes the conduct an offence. This applies to both the primary offence and ancillary offences. The effect of subsection 92A.2(2) is that the defendant will not be able to commit this offence overseas and avoid prosecution because the country in which he or she committed the offence does not have an offence that corresponds with section 92A.1.

Item 18

1150. Item 18 repeals existing section 93.1 regarding consent of the Attorney-General to the institution of proceedings and replaces it with a new section 93.1, which provides for the consent of the Attorney-General for offences against Part 5.2 of the Criminal Code, as amended by this Bill. Currently, Part 5.2 only contains the espionage offences in section 91.1. Consistent with the amendments in this Bill, Part 5.2 will contain the following offences:

- Espionage – Subdivision A of Division 91
- Espionage on behalf of a foreign principal – Subdivision B of Division 91

- Espionage-related offences – Subdivision C of Division 91
- Foreign interference – Subdivision B of Division 92
- Foreign interference involving foreign intelligence agencies – Subdivision C of Division 92
- Theft of trade secrets involving foreign government principal – Division 92A

Section 93.1 – Consent of Attorney-General required for prosecutions

1151. Section 93.1 requires the written consent of the Attorney-General to commence proceedings against a person for offences in Part 5.2 of the Criminal Code, and is intended to ensure that there is appropriate oversight of prosecutions. This is appropriate given the seriousness of offences in Part 5.2 and the fact that such prosecutions inherently raise national security or international considerations.

1152. 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 (CDPP) is not able to take into account under the *Prosecution Policy of the Commonwealth*.

1153. Section 93.1 provides the Attorney-General opportunity to receive advice from relevant agencies and other Ministers on sensitivities that might arise if proceedings are commenced for offences under Part 5.2, and provides opportunity for consideration of whether the prosecution could be detrimental to Australia's foreign relations and national security.

1154. Subsection 93.1(2) clarifies that the following steps can be taken towards preparing for proceedings, without the written consent of the Attorney-General having been given:

- a person may be arrested for the offence and a warrant for such an arrest may be issued and executed
- a person may be charged with the offence, and
- a person so charged may be remanded in custody or on bail.

1155. Given the seriousness of offences contained in Part 5.2 of the Criminal Code, it is appropriate that some measures towards commencing proceeds be permitted without the consent of the Attorney-General. The steps specified at subsection 93.1(2) are intended to ensure that law enforcement agencies can intervene to prevent a person from continuing to offend, promoting the protection of the Australian public and Australia's national interests.

1156. Subsection 93.1(3) provides that nothing in subsection 93.1(2) prevents the discharge of the accused if proceedings are not continued within a reasonable time. Australian common law recognises that a prosecution may be stayed where there is undue delay, to protect Australia's justice system from abuse of processes. The right to stay a prosecution also supports the Court's role in providing procedural fairness to a defendant, and helps maintain public confidence in the administration of justice. It is therefore appropriate that subsection 93.1(3) specify that the steps towards commencing proceedings as described at

subsection 93.1(2) do not prevent the discharge of the accused if proceedings are not continued within a reasonable time.

1157. Subsection 93.1(4) provides that the Attorney-General must consider whether the conduct constituting an offence against Part 5.2 of the Criminal Code might be authorised:

- for an offence against Subdivision A of Division 91 (espionage) – in a way mentioned in subsection 91.4(1)
- for an offence against Subdivision B of Division 91 (espionage on behalf of a foreign principal) – in a way mentioned in subsection 91.9(1)
- for an offence against Subdivision B of Division 92 (foreign interference) – in a way mentioned in section 92.5, and
- for an offence against Subdivision C of Division 92 (foreign interference involving foreign intelligence activities) – in a way mentioned in section 92.11.

1158. Each of these provisions provides defences to offences in Part 5.2. Therefore, the effect of subsection 93.1(4) is to ensure that the Attorney-General consider whether an accused's conduct might be authorised as described in a defence when considering whether to provide consent to prosecute.

Item 19

1159. Item 19 omits the words 'interest of the security or defence of the Commonwealth' from subsection 93.2(2) of the Criminal Code and substitutes the words 'interests of Australia's national security'. This reflects the repeal of the definition of 'security or defence' from the definitions in section 90.1 of the Criminal Code by Item 13 of Schedule 1.

1160. The effect of this change is that a judge or magistrate presiding over proceedings for an offence against Part 5.2 of the Criminal Code (as amended by Schedule 1) will be able to order hearings in camera (or other protections) if satisfied that it is in the interests of Australia's national security.

1161. ***National security*** is defined in section 90.4, to be inserted by Item 16 of Schedule 1.

Item 20

1162. Item 20 will add new provisions at the end of Division 93 relating to evidentiary certificates, fault elements for attempted espionage offences and alternative verdicts.

Section 93.3 – Evidentiary certificate

1163. Section 93.3 will enable the Attorney-General to sign an evidentiary certificate that, for the purpose of proceedings for an offence against Division 91 (espionage) or Division 92 (foreign interference), is prima facie evidence that the information or article specified in the certificate either:

- has, or had at a specified time, a security classification;

- has, or had at a specified time, a specified level of security classification;
- concerns Australia's national security; or
- concerns a particular aspect of Australia's national security.

1164. An evidentiary certificate creates a presumption as to the existence of the facts contained in the certificate which requires the defendant to disprove those matters. Accordingly, the evidentiary certificate will reverse the burden of proof.

1165. Evidentiary certificates issued under section 93.3 will be used to settle formal matters of fact (that the information or article concerns national security or is security classified) which may otherwise be difficult to prove under the normal rules of evidence.

1166. This is because matters concerning Australia's national security and security classified information can be said to be peculiarly within the knowledge of the Commonwealth. Further, allowing evidentiary certificates to be issued will protect sensitive information and technical capabilities without having a detrimental effect of the defendant's right to a fair trial.

1167. In such cases, it may be difficult to settle the question of whether the particular information has a security classification, or had a security classification at a particular time, by adducing admissible evidence. It would often be necessary to adduce the original document or information from which the information was drawn into evidence. The admission into evidence of additional security classified information may risk compounding the harm to essential public interests by providing the defendant with additional security classified information that they have no need to know, as well as risking the further exposure of that information.

1168. It would often be necessary to put in place additional controls to protect the security classified information, such as those available under the *National Security Information (Criminal and Civil Proceedings) Act 2004*, which may impose additional burdens on the prosecution, defendant and court. In cases where the question of whether the information is, or was at a particular time, security classified information is essentially formal in nature, the use of a *prima facie* evidentiary certificate would facilitate the settling of that question by avoiding the difficulty of adducing additional classified evidence and the resultant imposition of potentially burdensome obligations on the parties and court.

1169. Consistent with subsection 93.3(2) an evidentiary certificate will establish prima facie evidence in a proceeding for an offence against Division 91 (espionage) or Division 92 (foreign interference) as opposed to conclusive evidence that cannot be challenged by a court or a defendant. Therefore, the defendant can challenge the matters set out in an evidentiary certificate and will have the opportunity for contrary evidence to be adduced during a court proceeding. Importantly, an evidentiary certificate will not establish the weight or veracity of the evidence. This will remain a matter for the court to determine.

Section 93.4 – Fault elements for attempted espionage offences

1170. Section 93.4 provides that, despite subsection 11.1(3) of the Criminal Code, the fault element in relation to each physical element of an offence of attempting to commit an offence against Subdivision A of Division 91 (espionage) or Subdivision B of Division 91 (espionage

on behalf of a foreign principal), is the fault element in relation to that physical element of the relevant offence.

1171. Subsection 11.1(3) of the Criminal Code states that for the offence of attempting to commit an offence, intention and knowledge are fault elements in relation to each physical element of the offence attempted.

1172. The purpose of section 93.4 is to ensure that there are no barriers to prosecuting offenders in situations where a controlled operation has been undertaken under Part IAB of the Crimes Act and the defendant is dealing with substituted information (that, due to the intervention of law enforcement officers, does not concern national security) or with an undercover police officer posing as a foreign principal. It is not acceptable for it to be harder to prosecute an offence where law enforcement agencies intervened to ensure actual classified information was not passed to a foreign power by engaging in a controlled operation.

1173. Section 93.4 will disapply the automatic fault elements of intention or knowledge to an offence of attempting an offence against Subdivision A of Division 91 (espionage) or Subdivision B of Division 91 (espionage on behalf of a foreign principal), and specifies that the requisite fault element applying to each physical element of the relevant attempted offence is the ordinary fault element applicable to that physical element in the relevant offence.

1174. For example, to make out an offence against subsection 91.1(1) (espionage – dealing with information etc. concerning national security which is or will be made available to a foreign principal) one of the elements that the prosecution is must prove beyond reasonable doubt is that the defendant was reckless as to whether his or her conduct resulted in, or would result in the information being made available to a foreign principal or a person acting on behalf of a foreign principal (see paragraph 91.1(1)(d)). Applying subsection 11.1(3) of the Criminal Code to an offence of attempting to commit an offence against subsection 91.1(1), the prosecution would have to prove beyond reasonable doubt that the person knew that his or her conduct resulted in, or would result in the information being made available to a foreign principal or a person acting on behalf of a foreign principal.

1175. The effect of section 93.4 is that, for the purposes of an offence of attempting to commit an offence against subsection 91.1(1), the automatic application of knowledge as the fault element applicable to the physical element in section 91.1(1)(d) will not apply. Rather, the ordinary fault element applicable to that physical element – which is recklessness - will apply instead.

Section 93.5 – Alternative verdicts

1176. Subsection 93.5(1) provides that if the trier of fact is not satisfied that a person is guilty of an offence specific in column 1 (see table below) and is satisfied, beyond reasonable doubt, that the person is guilty of an offence against the corresponding offence specified in column 2 then it may find the person not guilty of the column 1 offence but guilty of the column 2 offence.

1177. Subsection 93.5(2) provides that subsection 93.5(1) only applies if the person has been accorded procedural fairness in relation to the finding of guilt for the relevant offence

specified in column 2.

Alternative verdicts		
Item	**Column 1** **For an offence against:**	**Column 2** **The alternative verdict is an offence against:**
1	subsection 91.1(1)	subsection 91.1(2)
2	subsection 91.2(1)	subsection 91.2(2)
3	subsection 91.6(1)	the underlying offence mentioned in paragraph 91.6(1)(a)
4	subsection 91.8(1)	subsection 91.8(2)
5	subsection 92.2(1)	subsection 92.3(1)
6	subsection 92.2(2)	subsection 92.3(2)
7	section 92.7	section 92.8
8	section 92.9	section 92.10

Item 21

1178. Item 21 will amend section 94.1 of the Criminal Code to remove the words 'or document which is made, obtained, recorded, retained, forged, possessed or otherwise' and replace them with 'document or other article which is'.

1179. Section 94.1 deals with forfeiture of items dealt with in contravention of Part 5.2. Item 10 of Schedule 1 includes a definition of ***deals*** in section 90.1. This definition will apply to the word 'dealt' in section 94.1, which allows the words 'made, obtained, recorded, retained, forged, possessed' to be repealed from the section.

Item 22

Section 132.8A – Damaging Commonwealth property

1180. Item 22 inserts a new section 132.8A after section 132.8 of the Criminal Code.

1181. Section 132.8A creates a new offence of damaging Commonwealth property to replace the existing offence of destroying or damaging Commonwealth property at section 29 of the Crimes Act, which will be repealed by Item 43 of Schedule 1.

1182. Section 132.8A creates an offence that applies where a person damages or destroys Commonwealth property. The offence will be punishable by a maximum penalty of 10 years imprisonment.

1183. An example of this offence is where Person A intentionally smashes the windscreens of a fleet of Commonwealth cars.

1184. To establish the offence, prosecution will need to prove beyond reasonable doubt that:

- the persons intentionally engages in conduct
- the person's conduct results in damage to, or the destruction of, property and the person is reckless as to this element, and

- the property belongs to a Commonwealth entity

1185. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 132.8A(1)(a). Under section 5.2 of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

1186. Recklessness is the fault element for paragraph 132.8A(1)(b). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and

- a result if he or she is 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 the risk.

1187. Absolute liability to paragraph 132.8A(1)(c) consistent with subsection 132.8A(2).

1188. For paragraph 132.8A(1)(a) of the offence, the prosecution will have to prove beyond a reasonable doubt that the defendant intentionally engaged in the relevant conduct. Consistent with subsection 4.1(2) of the Criminal Code, the reference to 'engages in conduct' in paragraph 132.8A(1)(a) means to do an act or to omit to perform an act.

1189. For paragraph 132.8A(1)(b) of the offence, the prosecution will have to prove beyond a reasonable doubt that the conduct resulted in damage to, or the destruction of, property. The terms damage, destruction and property are not defined and are intended to take their ordinary meaning. The prosecution will have to prove that the defendant is reckless as to the circumstance in paragraph 132.8A(1)(b). Therefore, the defendant must have been aware of a substantial risk that his or her conduct would result in damage to, or the destruction of, property and, having regard to the circumstances known to him or her it was unjustifiable to take that risk.

1190. The term damage is intended to have its ordinary meaning and would include conduct that impairs the value, usefulness, or normal functioning of the property, or have some other type of detrimental effect on the property.

1191. The term destruction is intended to include acts that cause so much damage that the property no longer exists, or cannot be repaired so that it is in its original state. The term could include the annihilation, obliteration, elimination or eradication of the property.

1192. The existing definition of ***property*** in section 130.1 will apply to the offence in section 132.8A. This definition includes:

- real property

- personal property

- money

- a think in action or other intangible property

- electricity
- a wild creature that is:
    - tamed
    - ordinarily kept in captivity, or
    - reduced (or in the course of being reduced) into the possession of a person.

1193. For paragraph 132.8A(1)(c) of the offence, the prosecution will have to prove beyond reasonable doubt that the property referred to in paragraph 132.8A(1)(b) belongs to a Commonwealth entity. This paragraph ties the offence to Commonwealth jurisdiction. For example, damage or destruction of property belonging to a State or Territory government would not be captured by the Commonwealth offence of damaging Commonwealth property.

1194. For the purposes of Chapter 7 of the Criminal Code, in which section 132.8A will be located, section 130.2 defines when property ***belongs to*** a person. Under section 130.2, property ***belongs to*** a person if, and only if:

- the person has possession or control of the property
- the person has a proprietary right or interest in the property, other than an equitable interest arising only from:
    - an agreement to transfer an interest
    - an agreement to grant an interest, or
    - a constructive trust.

1195. The term ***Commonwealth entity*** is defined in the Dictionary to the Criminal Code as the Commonwealth, or a Commonwealth authority.

1196. Subsection 132.8A(2) applies absolute liability to paragraph 132.8A(1)(c). Absolute liability is set out in section 6.2 of the Criminal Code. The effect of applying absolute liability to an element of an offence is that no fault element needs to be proved and the defence of mistake of fact is unavailable. Accordingly, for paragraph 132.8A(1)(c), the prosecution will be required to prove only the physical element that the property that has been damaged or destroyed belongs to a Commonwealth entity.

1197. Absolute liability is appropriate and required for the element of the offence that the right arises under the Constitution or a law of the Commonwealth because this element is a jurisdictional element of the offence. A jurisdictional element of the offence is an element that does not relate to the substance of the offence, but marks a jurisdictional boundary between matters that fall within the legislative power of the Commonwealth and those that do not. The issue of whether the person knew that the property they had damaged or destroyed was Commonwealth property is not relevant to their culpability. This is consistent with Commonwealth criminal law practice, as described in the Guide to Framing Commonwealth Offences.

1198. The application of absolute liability to paragraph 132.8A(1)(c) also ensures that a person cannot avoid criminal responsibility because they were unaware that the property they damaged or destroyed belongs to a Commonwealth entity, for example by admitting that they knew they had damaged or destroyed government property but thought that the property belonged to a State or Territory government.

1199. The application of absolute liability is also consistent with other Commonwealth property offences in Part 7.2 of the Criminal Code, including theft (section 131.1). Absolute liability applies to the element of the theft offence that the property belongs to a Commonwealth entity.

1200. Subsection 132.8A(3) applies Section 15.4 (extended geographical jurisdiction—Category D) to section 132.8A. Under section 15.4, the effect of Category D geographical jurisdiction is that the offence applies:

- whether or not the conduct constituting the alleged offence occurs in Australia, and
- whether or not a result of the conduct constituting the alleged offence occurs in Australia.

1201. Category D jurisdiction is appropriate because property belonging to a Commonwealth entity could be located outside of Australian territory. A common example is Australian Embassies and High Commissions located overseas. The application of Category D jurisdiction is also consistent with other Commonwealth property offences in Part 7.2 of the Criminal Code, including the theft offence at section 131.1.

1202. The maximum penalty of 10 years imprisonment is appropriate and consistent with the existing penalty for the offence of destroying or damaging Commonwealth property in section 29 of the Crimes Act. The maximum penalty also complements comparable offences in other Commonwealth legislation. For example, the offence of unauthorised modification of data to cause impairment at subsection 477.2 of the Criminal Code has a maximum penalty of 10 years imprisonment.

Item 23

1203. Item 23 amends subsection 132.7(5) of the Criminal Code to include a reference to the new offence of 'Damaging Commonwealth property' at section 132.8A(1) (as inserted by Item 22 of Schedule 1) to the list of property offences that form part of the offence of 'Going equipped for theft or a property offence' in section 132.7.

1204. This will mean that the offence at section 132.7 will be able to be committed by a person who, when not at home, has with him or her any article with intent to use it in the course of, or in connecting with, the offence of 'Damaging Commonwealth property' at new section 132.8A.

Item 24

1205. Item 24 amends the Dictionary to the Criminal Code to insert new definitions needed for the offences contained in Schedule 1.

Dictionary to the Criminal Code

1206. ***Constitutional trade or commerce*** is defined to mean trade and commerce:

- with other countries
- among the States
- between a State and a Territory, or
- between two Territories.

1207. This definition is consistent with the Commonwealth's power to legislate in relation to trade and commerce under the Constitution.

1208. ***Defence Minister*** is defined to mean the Minister administering the *Defence Force Discipline Act 1982.*

1209. ***Foreign intelligence agency*** is defined to mean an intelligence or security service (however defined) of a foreign country. This definition is intentionally broad to capture the range of intelligence agencies that exist in various countries, noting that some are controlled by government entities and others by political parties. International government and political organisations may also seek to establish and use intelligence agencies to further their objectives. Such agencies will generally, but not always, have comparable functions to agencies within the Australian Intelligence Community, as set out at the definition of ***domestic intelligence agency*** in section 121.1 of Schedule 2 of this Bill. This includes:

- the Australian Secret Intelligence Service
- ASIO
- the Australian Geospatial-Intelligence Organisation
- the Defence Intelligence Organisation
- the Australian Signals Directorate, and
- the Office of National Assessments.

1210. ***Mutiny*** is defined to have the meaning given by subsection 83.1(2), which defines mutiny as a combination between persons who are, or at least two of whom are, members of the Australian Defence Force:

- to overthrow lawful authority in the Australian Defence Force or in a force of another country that is acting in cooperation with the Australian Defence Force, or
- to resist such lawful authority in such a manner as to substantially prejudice the operational efficiency of the Australian Defence Force, or of a part of, a force of another country that is acting in cooperation with the Australian Defence Force.

Item 25

1211. Item 25 includes a savings provision that provides that if, immediately before the commencement of this item, a Proclamation is in effect for the purposes of paragraph 80.1AA(1)(b) of the Criminal Code as in force at that time, the Proclamation:

- continues in effect despite the repeal and substitution of section 80.1AA of the Criminal Code by Schedule 1, and
- has effect for the purposes of the Criminal Code as amended by this Schedule as if it had been made under section 80.1AB of the Criminal Code, as inserted by Schedule 1.

1212. Subitem (2) of Item 25 provides that subitem (1) does not prevent the Proclamation being repealed.

1213. This item allows any Proclamations made under section 80.1AA to continue to have effect once the provisions in Schedule 1 commence.

1214. No Proclamations have been made under section 80.1AA.

PART 2 – CONSEQUENTIAL AMENDMENTS

Aboriginal and Torres Strait Islander Act 2005

Item 26

1215. The *Aboriginal and Torres Strait Islander Act 2005* refers to the offence at section 28 of the Crimes Act (Interference with political liberty) in the definition of 'undue influence' at subclause 1(1) of Schedule 4.

1216. Section 28 will be repealed by Item 43 of Schedule 1. Item 8 will insert a new offence of 'Interference with political rights and duties' in section 83.4 of the Criminal Code.

1217. Item 26 will amend subclause 1(1) of the Schedule 4 to remove the reference to section 28 of the Crimes Act and substitute a reference to the new offence at section 83.4 of the Criminal Code.

Australian Citizenship Act 2007

Item 27

1218. Paragraph (a) of the definition of 'national security offence' in section 3 of the *Australian Citizenship Act 2007* refers to Part II of the Crimes Act, which will be repealed by Item 43 of Schedule 1.

1219. Item 8 of Schedule 1 inserts new Division 83 into Part 5.1 of the Criminal Code which creates new offences replacing Part II of the Crimes Act.

1220. Item 27 amends paragraph (a) of the definition of national security offence in section 3 to omit the reference to Part II of the Crimes Act. Item 28, below, inserts a

reference to Part 5.1 into the definition of 'national security offence' in section 3, which will ensure the new offences in Division 83 are covered by the definition.

Item 28

1221. Paragraph (c) of the definition of 'national security offence' in section 3 of the *Australian Citizenship Act 2007* refers to Parts 5.1, 5.2 or 5.3 of the Criminal Code.

1222. Item 28 repeals these references and replace them with references to:

- an offence against Part 5.1 of the Criminal Code (treason and related offences)
- an offence against Division 91 of the Criminal Code (espionage), and
- an offence against Part 5.3 (terrorism) of the Criminal Code.

1223. This amendment ensures that the definition of 'national security offence' continues to cover espionage, treason and other threats to security following the enactment of the new offences in Schedule 1.

Items 29 and 30

1224. Section 35A of the *Australian Citizenship Act 2007* empowers the Minister to determine in writing that a person ceases to be an Australian citizen if they commit one of the prescribed offences.

1225. Subparagraph 35A(1)(a)(ii) refers to sections 80.1 Treason), 80.1AA (Treason – materially assisting enemies etc.) and section 91 (Espionage) of the Criminal Code. These Following the amendments to these offences made by Schedule 1, Item 29 will repeal these references and replace them with references to:

- a provision of Subdivision B of Division 80 of the Criminal Code (treason)
- a provision of Division 82 of the Criminal Code (sabotage), and
- a provision of Division 91 of the Criminal Code (espionage).

1226. Subparagraph 35A(1)(a)(v) refers to sections 24AA (Treachery) and 24AB (Sabotage) of the Crimes Act. These offences will be repealed by Item 43 of Schedule 1. Item 4 of Schedule 1 will create a new Treachery offence in section 80.1AC of the Criminal Code. Item 8 of Schedule 1 will create new sabotage offences in Division 82 of the Criminal Code.

1227. Item 30 repeals subparagraph 35A(1)(a)(v) to remove the references to sections 24AA and 24AB of the Crimes Act. The new offences created by Items 4 and 8 of Schedule 1 will be covered by new subparagraphs (ii) and (iia), inserted by Item 28.

Australian Federal Police Act 1979

Items 31, 32, 33 and 34

1228. The definition of 'protective service offence' in section 4 of *the Australian Federal Police Act 1979* refers to section 24AB (sabotage) and section 28 (interfering with political liberty) of the Crimes Act, and section 91.1 (espionage) of the Criminal Code.

1229. Following the amendments made to those offences by Schedule 1, Items 31, 32, 33 and 34 will make minor amendments to update these references.

1230. Items 31 and 34 repeal references to section 24AB (sabotage) and section 28 (interfering with political liberty) of the Crimes Act and section 91.1 (espionage) of the Criminal Code. Item 32 replaces these references with references to:

- Division 82 of the Criminal Code (sabotage)
- Division 91 of the Criminal Code (espionage), and
- Section 132.8A of the Criminal Code (damaging Commonwealth property).

1231. Item 33 will make a minor grammatical change to accommodate the above amendments.

Commonwealth Electoral Act 1918

Item 35

1232. Item 35 updates the meaning of 'undue influence' in subsection 352(1) of the *Commonwealth Electoral Act 1918* to reflect the new offence of interference with political rights and liberties at section 83.4 of the Criminal Code (inserted by Item 8 of Schedule 1)

1233. If the Court of Disputed Returns finds that an elected candidate has committed or attempted to commit bribery or undue influence, the election of the candidate will be declared void under section 362 of the Commonwealth Electoral Act. Bribery means a contravention of section 326 of the Commonwealth Electoral Act.

1234. Convictions for bribery or undue influence also disqualify a person from candidature for either federal House of the Parliament for two years under section 386 of the Commonwealth Electoral Act.

1235. In the context of the Commonwealth Electoral Act, convictions under section 83.4 that relate to electoral matters (such as the right to vote, the right to stand as a candidate and the right to support or oppose a candidate, group of candidates or party, would be relevant for the purposes of the definition of 'undue influence'.

Item 36

1236. Section 386 of the Electoral Act provides that convictions for bribery or undue influence (or their attempt) disqualify a person from candidature for either federal House of the Parliament for two years from the date of the conviction.

1237. Item 36 updates the reference in subparagraph 386(a)(i) of the *Commonwealth Electoral Act 1918* to refer to new section 83.4 of the Criminal Code (to be inserted by Item 8 of Schedule 1).

Crimes Act 1914

Item 37

1238. Section 4J of the Crimes Act deals with offences that may be dealt with summarily. Subsection 4J(7) provides that offences against: section 24AA (treachery), section 24AB (sabotage) and subsections 79(2) and (5) (secrecy) of the Crimes Act and Division 80 (treason) and section 91.1 (espionage) of the Criminal Code may not be dealt with summarily.

1239. Following the amendments to these offences made by Schedule 1, Item 37 updates subsection 4J(7) of the Crimes Act to refer to the new offences against:

- subsections 79(2) or (5) of the Crimes Act
- Division 80 of the Criminal Code (treason, urging violence and advocating terrorism or genocide)
- Division 82 of the Criminal Code (sabotage)
- Division 91 of the Criminal Code (espionage), and
- Division 92 of the Criminal Code (foreign interference).

1240. The effect of this is that offences against these provisions may not be dealt with summarily. This is appropriate due to the seriousness of these offences.

1241. Item 5 of Schedule 2 will repeal subsections 79(2) and (5) from the Crimes Act. Item 4 of Schedule 2 will therefore repeal the reference to these subsections from the subsection 4J(7). As Schedule 2 commences on a single day to be set by Proclamation, this item ensures that subsection 4J(7) continues to cover the offences in subsection 79(2) and (5) until such time as they are repealed.

Items 38 and 39

1242. Section 15AA of the Crimes Act provides that bail must not be granted to a person charged with, or convicted of, an offence listed in subsection 15AA(2) unless exceptional circumstances exist. Subsection 15AA(2) refers to existing Subdivision C of Division 80 (urging violence and advocating terrorism or genocide) and Division 91 (offences relating to espionage and similar activities) of the Criminal Code and section 24AA (treachery) of the Crimes Act.

1243. Item 38 repeals these references and updates them with references to the new provisions in Division 80 (treason, urging violence and advocating terrorism or genocide) or Division 91 (espionage) of the Criminal Code.

1244. Item 39 will add the new foreign interference offences in subsection 92.2(1) and subsection 92.3(1) of the Criminal Code to section 15AA(2) of the Crimes Act, but only

where it is alleged that the defendants conduct in relation to the offence involved making a threat to cause serious harm or a demand with menaces. Expanding section 15AA(2) in this way is appropriate given that the conduct is similar in nature to that of an espionage offence. However, it is appropriate that a person being prosecuted for a foreign interference offence against section 92.2(1) and 92.3(1) should only be subject to a presumption against bail in circumstances when there is a threat of harm.

Items 40 and 41

1245. Part IAE of the Crimes Act deals with the use of video link evidence in proceedings for terrorism and related offences. The purpose of the video link provisions is to facilitate the prosecution of terrorism and related offences by ensuring that, in the absence of compelling reasons to the contrary, important evidence from overseas witnesses who are unable to travel to Australia can be put before the court using video link technology.

1246. Existing section 24AA (treachery) and section 24AB (sabotage) are included as proceedings to which Part IAE applies under paragraph 15YU(1)(g).

1247. Items 40 and 41 make minor amendments to section 15YU of the Crimes Act to update these references with references to Subdivision B of Division 80 (Treason) and Division 82 (sabotage) of the Criminal Code.

Item 42

1248. Paragraph 19AG(1)(a) of the Crimes Act, which deals with minimum non-parole periods, currently refers to section 24AA (treachery) of the Crimes Act.

1249. Section 24AA is being repealed by Item 43 of Schedule 1.

1250. Item 42 will repeal section 19AG(1)(a). The offence replacing section 24AA (section 80.1AC of the Criminal Code, to be inserted by Item 4 of Schedule 1), will be covered by the existing reference to Division 80 of the Criminal Code in subsection 19AG(1)(c).

Item 43

1251. Item 43 repeals Part II of the Crimes Act. The offences within this Part are moved to the Criminal Code (see Division 83, inserted by Item 4 of this Schedule) as indicated by the following table

Crimes Act	Criminal Code
Section 24AA – Treachery	Section 80.1AC
Section 24AB – Sabotage	Division 82
Section 25 – Inciting mutiny	Section 83.1
Section 26 – Assisting prisoners of war to escape	Section 83.2
Section 27 – Unlawful drilling	Section 83.3
Section 28 – Interfering with political liberty	Section 83.4
Section 29 – Destroying or damaging Commonwealth property	Section 132.8A

Foreign Evidence Act 1994

Item 44

1252. Item 44 amends the definition of 'designated offence' in section 3 of the *Foreign Evidence Act 1994* to refer to the new sabotage offences in Division 82 of the Criminal Code, to be inserted by Item 8 of Schedule 1.

1253. The definition of 'designated offence' under section 3 of the currently refers to the sabotage offence in section 24AB of the Crimes Act 1914 (paragraph (g)), which is being repealed by item 43 of this Schedule.

1254. Item 44 amends section 3 to insert a new paragraph referring to an offence against Division 82 (sabotage).

1255. Part 3A of the Foreign Evidence Act provides that evidence from other countries can be used in Australian criminal and civil terrorism-related proceedings. It establishes procedures for enabling authenticated foreign testimony and exhibits to such testimony to be admissible, subject to appropriate safeguards. 'Terrorism-related proceedings' is defined in section 3 of the Foreign Evidence Act to include 'designated offences.' For the purposes of Part 3A, 'foreign material' includes testimony of a person and associated exhibits, and 'Foreign government material' includes material provided by a foreign authority to the Commonwealth.

1256. This item will ensure the definition of 'designated offence' in the Foreign Evidence Act includes the new proposed sabotage offences. It will mean that material received from foreign countries, including on an agency-to-agency basis (for example, through police or intelligence channels), can be adduced by prosecutors and responsible authorities in sabotage-related proceedings, in accordance with Part 3A of the Foreign Evidence Act. It is appropriate that material obtained overseas relating to these new offences can be provided to a court as evidence in terrorism-related proceedings.

1257. There are strict safeguards in the Foreign Evidence Act for how material is dealt with in terrorism-related proceedings. Subsection 27C(2) of the Foreign Evidence Act provides the Court with a broad judicial discretion to prevent material from being adduced if it would have a substantial adverse effect on the right of another party to the proceeding to receive a fair hearing. Subsection 27D(2) provides an exception to admissibility if the material or information contained in the material was obtained directly because of torture or duress. In accordance with section 27DA, following a request by a party, the presiding judge in a terrorism-related proceeding in which foreign material has been admitted, can warn the jury about the reliability of that evidence.

Item 45

1258. Item 45 repeals paragraph (g) of the definition of 'designated offence' in section 3 of the *Foreign Evidence Act 1994*, to remove references to section 24AA (treachery) and section 24AB (sabotage) of the Crimes Act, which will be repealed by Item 43 of Schedule 1.

1259. Treachery and sabotage offences will continue to be captured under the definition of 'designated offence' in the Foreign Evidence Act. Item 44 inserts a reference to the proposed sabotage offences at Division 82 of the Criminal Code. The updated treachery offence

(section 80.1AC of the Criminal Code) will be captured through paragraph (da) of the definition of 'designated offence.'

Migration Act 1958

Items 46, 47 and 48

1260. Section 203 of the *Migration Act 1958* deals with deportation of non-citizens who are convicted of certain serious offences.

1261. Under subparagraph 203(1)(c), offences against sections 24AA (treachery), 24AB (sabotage), 25 (inciting mutiny) and 26 (assisting prisoners of war to escape) of the Crimes Act are listed. These offences will all be repealed by Item 43 of Schedule 1. Following the amendments to these offences by Schedule 1 of the Bill, Items 46, 47 and 48 will repeal these references from subparagraph 203(1)(c)(i) and replace them with references to:

- Division 82 (sabotage) of the Criminal Code
- section 83.1 (advocating mutiny) of the Criminal Code, and
- section 83.2 (assisting prisoners of war to escape) of the Criminal Code, and
- a provision of Subdivision B of Division 80 of the Criminal Code.

1262. The reference to section 24AA(treachery) will not be replaced, as the new treachery offence in section 80.1AC (to be inserted by Item 4 of Schedule 1) is covered by the reference to Division 80 of the Criminal Code that already exists in subparagraph 203(1)(c)(ia).

Surveillance Devices Act 2004

Items 49 and 50

1263. Section 30 of the *Surveillance Devices Act 2004* deals with emergency authorisation procedures for use of a surveillance device. Under this provision, where a law enforcement officer reasonably suspects that the use of a surveillance device is immediately necessary to prevent the loss of any evidence relevant to an investigation of a specified offence and it is not practicable to obtain a warrant from an eligible judge or nominated AAT, that officer may apply for an emergency authorisation. Subparagraph 30(a)(vi) contains a reference to section 91.1 (espionage and similar activities) of the Criminal Code as one of the offences to which an emergency authorisation is available.

1264. Items 49 and 50 amend subparagraph 30(1)(a)(vi) of the Surveillance Devices Act to ensure that this power is available to the extended range of espionage related offences in Division 91 of the Criminal Code.

1265. It is important that law enforcement officers be able to obtain evidence of the commission of espionage-related activity in an efficient manner. Given the nature of these offences, it is often difficult to investigate them by other means, particularly as offenders habitually attempt to conceal any wrongdoing. In these circumstances the urgent deployment of a surveillance device will be necessary to prevent loss of evidence. Emergency

authorisations must be retrospectively approved by an eligible Judge or nominated AAT member within 48 hours of issue.

SCHEDULE 2 – SECRECY

General Outline

1266. Schedule 2 introduces new Part 5.6 and Division 122 into the Criminal Code. New Part 5.6 contains a suite of new Commonwealth secrecy offences. These new offences replace sections 70 and 79 of the Crimes Act and will apply if the information disclosed is inherently harmful (such as security classified information) or would otherwise cause harm to Australia's interests. The offences will apply to all persons, not just Commonwealth officers. New Division 122 includes defences to ensure the offences do not apply too broadly, including a defence specifically applying to journalists engaged in fair and accurate reporting in the public interest.

PART 1 – SECRECY OF INFORMATION

Crimes Act 1914

Items 1 and 2

1267. These items amend the definition of ***Commonwealth officer*** in subsection 3(1) of the Crimes Act, to omit the definition of the term for the purposes of section 70 of the Crimes Act, which is currently contained in paragraphs (c) and (d). Item 5 of Schedule 2 repeals section 70 of the Crimes Act, making the definition unnecessary.

Item 3

1268. Item 3 repeals the definition of ***Queen's dominions*** in subsection 3(1) of the Act. This term was used only in section 79 of the Crimes Act. Item 5 of this Schedule repeals section 79 of the Crimes Act, making the definition unnecessary.

Item 4

1269. Section 4J of the Crimes Act provides for circumstances in which certain indictable offences against the law of the Commonwealth may be heard and determined by a court of summary jurisdiction. Paragraph 4J(7)(a) currently provides that, notwithstanding the effect of section 4J, offences against sections 24AA (Treachery) or 24AB (Sabotage), or subsections 79(2) and (5) (being official secrets offences punishable by seven years' imprisonment) of the Crimes Act may not be tried summarily.

1270. Item 4 repeals paragraph 4J(7)(a) of the Crimes Act. Item 43 of Schedule 1 of the Bill repeals sections 24AA and 24AB, and Item 5 of this Schedule repeals section 79, making this paragraph unnecessary.

Item 5

1271. Item 5 repeals Parts VI and VII of the Crimes Act.

1272. Part VI of the Crimes Act (Offences by and against public officers) contains one secrecy offence (section 70) that applies where Commonwealth officers disclose information that he or she is under a duty not to disclose. Section 70 does not create a duty of non-disclosure for Commonwealth officials. Rather, section 70 operates to establish a criminal offence for Commonwealth officials who breach a pre-existing duty of confidence.

1273. For example, subregulation 2.1(3) of the *Public Service Regulations 1999* imposes a duty on Australian Public Service employees to not disclose information which the APS employee generates in connection with their employment in certain circumstances. Subregulation 2.1(3) is not an offence provision. However, by establishing a duty of non-disclosure, the subregulation enlivens the offence provision in section 70.

1274. The drafting of section 70 is outdated and complicated, resulting in a lack of clarity about the scope of the offence. For example, section 70 will be enlivened where a Commonwealth official is subject to a duty of non-disclosure arising elsewhere. It is well-established that a statutory duty of non-disclosure may enliven the offence. Comparatively, it remains unresolved whether a duty at common law or in equity would be a relevant duty for the purposes of the offence. Similarly, the offence requires the disclosure of a 'fact or document'. The application of the offence to the disclosure of factual information or documents is well-established, however there is some uncertainty about the application of the offence to the disclosure by a Commonwealth official of matters of opinion or advice that are not factual in nature in a non-documentary form.

1275. Part VII of the Crimes Act (Official secrets and unlawful soundings) contains a range of offences relating to official secrets, prohibited places and unlawful soundings. The Part also contains a range of procedural provisions.

1276. There have been calls for significant reforms to Parts VI and VII for many years. In particular, the Australian Law Reform Commission's 2010 Report, *Secrecy Laws and Open Government in Australia* (Report 112) concluded that there are 'real concerns' with the operation of the existing offences, which are 'out of step with public policy developments in Australian and internationally'. Additionally, the drafting of the current offences is outmoded. As a result, it can be challenging for persons to understand when they will be subject to criminal liability, and for bring successful prosecutions.

Item 6

1277. Item 6 inserts a new Part 5.6 to the Criminal Code, entitled 'Secrecy of information'. New Part 5.6 will contain the new general secrecy offences, replacing Parts VI and VII of the Crimes Act.

Division 121—Preliminary

1278. New Division 121 of the Criminal Code contains definitions relating to the new general secrecy offences, as well as an evidentiary certificate framework.

Section 121.1—Definitions

1279. Item 6 inserts the following new definitions relevant to the secrecy offences in section 122.1 of the Criminal Code:

- cause harm to Australia's interests
- Commonwealth officer
- deal

- domestic intelligence agency
- information
- inherently harmful information
- international relations
- proper place of custody
- Regulatory Powers Act
- security classified information, and
- security or defence of Australia

Definition of 'cause harm to Australia's interests'

1280. Item 6 inserts a new definition of ***cause harm to Australia's interests*** for the purposes of Part 5.6 of the Criminal Code. The phrase is used as part of the elements of the new general secrecy offence in section 122.2, relating to conduct causing harm to Australia's interests. The definition contains an exhaustive list of matters which represent essential national interests. Causing harm to these interests is a serious matter which, in certain circumstances set out in section 122.2, should attract criminal liability.

1281. In its 2010 report, *Secrecy Laws and Open Government in Australia*, the Australian Law Reform Commission recommended that (Recommendation 5-1):

> The general secrecy offence should require that the disclosure of Commonwealth information did, or was reasonably likely to, or intended to:
> a. damage the security, defence or international relations of the Commonwealth;
> b. prejudice the prevention, detection, investigation, prosecution or punishment of criminal offences;
> c. endanger the life or physical safety of any person; or
> d. prejudice the protection of public safety.

1282. Paragraphs (a), (c), (d), and (g) of the definition correspond with the categories of harm recommended by the ALRC.

1283. Paragraph (a) provides that causing harm to Australia's interests includes interfering with or prejudicing the prevention, detection, investigation, prosecution and punishment of criminal offences against the law of the Commonwealth, and contraventions of laws of the Commonwealth that are subject to civil penalties.

1284. The inclusion of interfering with or prejudicing the prevention, detection, investigation, prosecution and punishment of contraventions of Commonwealth civil penalty provisions goes beyond the ALRC's recommendation. When read together with the offence provision in section 122.2, the use of official information to interfere with or prejudice the effective enforcement of a civil penalty provision involves a serious interference with the administration of justice, as well as an improper use of official information that is likely to undermine public confidence in the effective administration of justice. Accordingly, such conduct should be subject to criminal liability.

1285. The inclusion of the concepts of preventing, detecting, investigating, prosecuting and punishing Commonwealth criminal offences and contraventions of Commonwealth civil penalty provisions is intended to reflect the fact that the effective enforcement of the law and the maintenance of public order require the undertaking of a wide range of activities. Similarly, paragraph (a) is not restricted to interfering with or prejudicing the performance of the functions of a particular agency in relation to these matters. A range of agencies, bodies and persons may be involved in preventing, detecting or investigating an offence or contravention of a civil penalty provision, beyond those agencies directly responsible for the enforcement of the criminal law or a relevant civil penalty provision.

1286. Paragraph (b) provides that causing harm to Australia's interests includes interfering with or prejudicing the performance of the functions of the Australian Federal Police under:

- paragraph 8(1)(be) of the *Australian Federal Police Act 1979* (protective and custodial functions), or
- the *Proceeds of Crime Act 2002*.

1287. In relation to subparagraph (b)(i) of the definition, the AFP Act provides a function for the AFP in relation to perform protective and custodial functions. The AFP's protection operations function ensures the safety of individuals and interests deemed by the Commonwealth to be at risk from acts of terrorism, crime and issue-motivated violence. This includes protection within Australia and overseas to designated Australian and foreign dignitaries, internationally protected persons and visiting foreign dignitaries; planning and provision of security for major events; and uniform protection of designated Commonwealth establishments and diplomatic and consular missions within Australia and overseas. Protection of these individuals and interests is essential for national security.

1288. In relation to subparagraph (b)(ii) of the definition, the POCA establishes a civil forfeiture scheme to confiscate unlawfully acquired property, as well as associated powers such as asset freezing. Strong and effective action to confiscate proceeds of crime assists in attacking the profit-motive of organised crime, including illicit activities involving drug trafficking, people smuggling, money laundering and large-scale fraud. The effective performance of the Australian Federal Police's functions under the POCA is an essential public interest.

1289. The inclusion of interfering with or prejudicing proceeds of crime investigations under paragraph (b) goes beyond the ALRC's recommendation. The ALRC considered that it would be more appropriate to rely on specific secrecy provisions in sections 210, 217 and 223 the POCA (which relate to the unauthorised disclosure of information about production orders, notices to financial institutions and monitoring orders). However, those specific secrecy provisions cover only a subset of the kinds of official information that could be improperly communicated to interfere with or prejudice the performance of the Australian Federal Police's functions under the POCA, and the associated, essential public interests.

1290. Paragraphs (c) and (d) deal with harming or prejudicing Australia's international relations.

1291. Paragraph (c) provides that causing harm to Australia's interests includes harming or prejudicing Australia's international relations in relation to information that was communicated in confidence:

- by, or on behalf of, the government of a foreign country, an authority of the government of a foreign country or an international organisation, and

- to the Government of the Commonwealth, an authority of the Commonwealth or a person receiving the communication on behalf of the Commonwealth or the authority of the Commonwealth.

1292. For the avoidance of doubt, the information referred to in paragraph (c) of the definition is the information that is disclosed under section 122.2.

1293. The concepts of a person communicating information 'on behalf of' the government of a foreign country, an authority of the government of a foreign country, or an international organisation, and a person receiving a communication 'on behalf of' the Government of the Commonwealth or an authority of the Commonwealth should be interpreted broadly. It should include any person who communicates or receives information in an official or unofficial capacity on behalf of such a government, authority or organisation. This could include, for example:

- an officer, official or envoy of a government, however described

- a lawyer or agent engaged to represent a government, authority or organisation, who communicates or receives information on behalf of his or her client, or

- a person (including a contractor, employee of a contractor, subcontractor or employee of a subcontractor) engaged to perform work for a government, who communicates or receives information on behalf of the government.

1294. The requirement in paragraph (c), that a person's conduct must harm or prejudice Australia's international relations in relation to information that was communicated in confidence by a foreign government or international organisation to the Commonwealth, is consistent with the ALRC's view that not all disclosures of confidential information will cause harm, and that confidential information should only be protected by a general secrecy offence in cases where its disclosure would cause harm.

1295. Paragraph (d) provides that causing harm to Australia's interests includes harming or prejudicing Australia's international relations in any other way.

1296. Consistent with Recommendation 5-2 of the ALRC's report, the term 'international relations' is defined as having the meaning given in section 10 of the *National Security Information (Criminal and Civil Proceedings) Act 2004*. Section 10 of the NSI Act defines international relations to mean 'political, military and economic relations with foreign governments and international organisations'.

1297. The offences in section 122.2 will therefore apply where a person is aware of a substantial risk that their conduct will or is likely to harm or prejudice Australia's political, military or economic relations with foreign governments and international organisations, and having regard to the circumstances known to him or her, it is unjustifiable to take the risk.

1298. The concept of harming or prejudicing Australia's international relations includes such things as:

- the lessening or cessation of military or intelligence cooperation
- damage to Australia's negotiating position in respect of a treaty or agreement, or within an international organisation such as the United Nations or an organ thereof
- a reduction in the quality or quality of information provided by a foreign government or international organisation
- loss of confidence or trust in the Australian Government by an overseas government or international organisation
- a detrimental impact on the ability of the Australian Government to maintain good working relations with a foreign government or international organisation, or
- intangible damage to Australia's reputation or relationships between the Australian Government and a foreign government or international organisation, or between officials,

having the effect of diminishing the capacity of the Australian Government to function in the global political, military and economic environment.

1299. For the purposes of paragraph (c) of the definition, it is immaterial whether the harm or damage to Australia's international relations relates to the particular foreign government or international organisation who provided the information in question to the Australian Government in confidence. It is likely, for example, that the unauthorised communication of information given to the Australian Government in confidence by one foreign government would reduce the confidence or trust that multiple foreign governments and international organisations would have in the Australian Government's ability to protect each of those governments' and organisations' information.

1300. Paragraph (e) of the definition provides that causing harm to Australia's interest includes harming or prejudicing relations between the Commonwealth and a State or Territory. The concept of harming or prejudicing relations between the Commonwealth and a State or Territory includes things such as:

- the lessening or cessation of law enforcement cooperation
- a reduction in the quality or quality of information provided by a State or Territory
- loss of confidence or trust in the Commonwealth Government by a State or Territory Government
- a detrimental impact on the ability of the Commonwealth Government to maintain good working relations with a State or Territory Government, or

- intangible damage to Australia's reputation or relationships between the Commonwealth Government and a State or Territory Government, or between officials

having the effect of diminishing the capacity of the Commonwealth Government, or State or Territory Government, to function within Australia's federal structure.

1301. Paragraph (f) of the definition provides that causing harm to Australia's interest includes harming or prejudicing the health or safety of the public or a section of the public. The unauthorised communication of, or dealing in, official information that threatens public safety, or that threaten public health, are serious matters warranting criminal liability.

Definition of Commonwealth officer

1302. Item 6 inserts a new definition of ***Commonwealth officer***. The definition of Commonwealth officer forms part of the element of each of the offences in Division 122, and the defence in section 122.5. A person will only commit an offence under Division 122 for engaging in relevant conduct in relation to information if the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity. The definition contains an exhaustive list of individuals who are Commonwealth officers.

1303. Paragraph (a) of the definition provides that a Commonwealth officer includes an APS employee. The term APS employee should be interpreted consistently with section 2B of the Acts Interpretation Act provides that, in any Act, the term APS employee has the same meaning as in the *Public Service Act 1999*, being a person engaged under section 22 of that Act (Engagement of APS employees), or a person who is engaged as an APS employee under section 72 of that Act (Machinery of government changes).

1304. 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*.

1305. Paragraphs (c) and (d) of the definition provide that a Commonwealth officer includes a member of the Australian Defence Force and a member or special member of the Australian Federal Police. These terms are to be interpreted consistently with the definitions in the Defence Force Discipline Act and the *Australian Federal Police Act 1979*.

1306. Paragraph (e) of the definition provides that a Commonwealth officer includes an officer or employee of a ***Commonwealth authority***. The term ***Commonwealth authority*** is

defined in the Dictionary to the Criminal Code and means a body established by or under a law of the Commonwealth, subject to certain exceptions including for a body established under the *Corporations Act 2001*.

1307. Paragraphs (f) and (g) of the definition provide that a Commonwealth officer includes an individual who is a contracted service provider for a Commonwealth contract, as well as an individual who is an officer or employee of a contracted service provider for a Commonwealth contract and who provides services for the purposes (whether direct or indirect) of the Commonwealth contract.

1308. The term ***Commonwealth contract*** is defined in the Dictionary to the Criminal Code to mean a contract, to which a Commonwealth entity is a party, under which services are to be, or were to be, provided to a Commonwealth entity.

1309. ***Contracted service provider*** for a Commonwealth contract is defined in the Dictionary to the Criminal Code to mean:

- a person who is a party to the Commonwealth contract and who is responsible for the provision of services to a Commonwealth entity under the Commonwealth contract, or

- a subcontractor for a Commonwealth contract.

1310. The limitation, in paragraph (g), that the individual must provide services for the purposes (whether direct or indirect) of the Commonwealth contract ensures that a person who is an officer or employee of a contracted service provider in a role entirely unrelated to the Commonwealth contract is not a Commonwealth officer.

Definition of deal

1311. This item inserts a new definition of ***deal*** for the purposes of Part 5.6 of the Criminal Code. The term ***deal***, in Part 5.6, has the same meaning as in subsection 90.1(1) of the Criminal Code.

1312. Under section 90.1, a person ***deals*** with information or an article if the person does any of the following in relation to the information or article:

- receives or obtains it

- collects it

- possesses it

- makes a record of it

- copies it

- alters it

- conceals it

- communicates it

- publishes it, or
- makes it available.

Definition of domestic intelligence agency

1313. This item inserts a new definition of ***domestic intelligence agency*** for the purposes of Part 5.6 of the Criminal Code.

1314. The term is defined as meaning the six agencies that are members of the Australian Intelligence Community, being the Australian Secret Intelligence Service, Australian Security Intelligence Organisation, Australian Geospatial-Intelligence Organisation, Defence Intelligence Organisation, Australian Signals Directorate, and the Office of National Assessments.

Definition of information

1315. This item inserts a new definition of ***information*** for the purposes of Part 5.6 of the *Criminal Code*. The term has the same meaning given by section 90.1 of the Criminal Code, being means information of any kind, whether true or false and whether in a material form or not, and includes an opinion, and a report of a conversation.

1316. At present, the general secrecy offence in section 70 of the Crimes Act applies only in relation to facts or documents. The inclusion of definition of ***information*** will ensure that the new general secrecy offences in Division 122 apply in relation to opinion and advice that are not in documentary form. It will also ensure that the offences apply in relation to information that, while factually mistaken, is nevertheless inherently harmful information, or the disclosure of which would cause harm to Australia's interests.

1317. An example of the latter category of information would be an assessment produced by an Australian agency about a weapon system that may pose a threat to Australian forces that is factually mistaken about the capabilities of that system—the disclosure of that assessment would be inherently harmful, as it would, or would be reasonably expected to, allow the operator of the weapon system to exploit the Australian Defence Force's misunderstanding of the weapon system's capabilities.

1318. The alignment of the definition of information between Part 5.2 (Offences relating to espionage and similar activities) and Part 5.6 of the Criminal Code will also ensure that the espionage and secrecy offences apply to information consistently.

Definition of inherently harmful information

1319. This item inserts a new definition of ***inherently harmful information*** for the purposes of Part 5.6 of the *Criminal Code*. The definition exhaustively lists categories of information that are inherently harmful, in the sense that:

- communicating such information;
- otherwise dealing in such information;
- removing such information from, or holding such information outside, a proper place of custody for the information; or

- failing to comply with a lawful direction regarding the retention, use or disposal of such information,

will, or would reasonably be expected to, cause harm to essential public interests of the Commonwealth.

1320. Section 122.1 establishes a suite of new general secrecy offences, in respect of certain conduct relating to inherently harmful information made or obtained by a Commonwealth officer or person otherwise engaged to perform work for a Commonwealth entity. The offences in section 122.1 do not contain a harm element, as they relate to information that is inherently harmful.

1321. Paragraph (a) of the definition of provides that security classified information is a category of inherently harmful information. ***Security classified information*** is separately defined in section 121.1 as information that has a security classification, within the meaning of section 90.5 of the Criminal Code. Subsection 90.5(1) provides that ***security classification*** has the meaning prescribed by the regulations.

1322. The Commonwealth has well-established processes for determining whether particular information has been properly security classified, or remains appropriately security classified. These processes involve the review of the information by one or more persons who are familiar with the underlying reasons for the security classification, and well-placed to determine whether its classification 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 etc. of 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.

1323. Paragraph (b) of the definition provides that information the communication of which would or could reasonably be expected to, damage the security or defence of Australia is a category of inherently harmful information. The Commission recommended that such information be covered by a general secrecy offence (Recommendation 5-1).

1324. Paragraph (c) of the definition provides that information that was obtained by, or made by or on behalf of, a domestic intelligence agency or a foreign intelligence agency in connection with the agency's functions, is a category of inherently harmful information.

1325. The compromise of information made or obtained by the intelligence services could reasonably be expected to cause serious damage to Australia's national security. Even small amounts of such information could, when taken together with other information, compromise national security, regardless of the apparent sensitivity of the particular information—this is referred to as the 'mosaic approach' to intelligence collection.

1326. For example, even seemingly innocuous pieces of information, such as the amount of leave available to staff members or their salary, can yield significant counterintelligence dividends to a foreign intelligence service.

1327. 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.

1328. 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.

1329. Paragraph (e) of the definition provides that information relating to the operations, capabilities and technologies of, and methods and sources used by, a domestic or foreign law enforcement agency is a category of inherently harmful information. A person will not be subject for criminal liability for communicating etc. such information in circumstances covered by the defences in section 122.4. These circumstances include where the information has already been communicated or made available to the public with the authority of the Commonwealth. A person would not be subject to liability for communicating information about a law enforcement operation that has been made available to the public with the authority of the Commonwealth, for example, because the operation was conducted in public. The concept of making information available to the public includes making information to a relevant segment of the public, and can include making information available to a single person, for example where an operation is conducted in public but witnessed only by a single person.

1330. A defence is also available where a person communicated the information in the public interest, and in the person's capacity as a journalist engaged in fair and accurate reporting.

1331. Paragraph (e) of the definition provides that information relating to the operations, capabilities or technologies of, or methods or sources used by, a domestic or foreign law enforcement agency is a category of inherently harmful information. The unauthorised disclosure of law enforcement 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.

1332. The scope of information covered by paragraph (e) in relation to law enforcement agencies is substantially narrower than the scope of information covered by paragraph (c), in relation to intelligence agencies. Paragraph (e) will only cover information relating to the operations, capabilities and technologies of, and methods and sources used by, a law enforcement agency. It is not intended that paragraph (e) will generally cover include information such as the identity of law enforcement officers (other than officers operating under assumed identities), their salaries, or locations of their facilities.

1333. A person will not be subject for criminal liability for communicating or otherwise dealing with information covered by paragraph (e) in circumstances covered by the defences in section 122.5. In particular, subsection 122.5(2) provides that it is a defence to a prosecution for an offence relating to the communication or dealing with inherently harmful information that the information has already been communicated or made public with the authority of the Commonwealth. It is intended that a person would not be subject to criminal liability for communicating information about a law enforcement operation that has been made available to the public with the authority of the Commonwealth, for example, because the operation was conducted in public. The concept of making information available to the public includes making information to a relevant segment of the public, and can include making information available to a single person, for example where an operation is conducted in public but witnessed only by a single person. As a result, the inclusion of law enforcement operations within the definition of inherently harmful information is not intended to have the effect of extending criminal liability to persons who communicate information about public law enforcement operations.

Definition of international relations

1334. This item inserts a new definition of ***international relations*** for the purposes of Part 5.6 of the Criminal Code. The term is used as part of the definition of ***causes harm to Australia's interests***, a subset of which is to harm or prejudice Australia's international relations.

1335. Consistent with Recommendation 5-2 of the ALRC's report, the term 'international relations' is defined as having the meaning given in section 10 of the *National Security Information (Criminal and Civil Proceedings) Act 2004*. The NSI Act defines international relations to mean 'political, military and economic relations with foreign governments and international organisations'.

1336. The offence provisions in section 122.2 will, therefore, apply where the information falls within this definition and a person is aware of a substantial risk that their conduct will or is likely to harm or prejudice Australia's political, military or economic relations with foreign governments and international organisations, and having regard to the circumstances known to him or her, it is unjustifiable to take the risk.

Definition of proper place of custody

1337. This item inserts a new definition of ***proper place of custody*** for the purposes of Part 5.6 of the *Criminal Code*. The term is used as part of the offence provisions in Division 122, which provide that it is an offence in certain circumstances for a person to intentionally remove information from a proper place of custody, or to hold information outside a proper place of custody.

1338. The term proper place of custody has the meaning given in section 121.2 (Definition of proper place of custody).

Definition of Regulatory Powers Act

1339. This item inserts a new definition of ***Regulatory Powers Act*** for the purposes of Part 5.6 of the *Criminal Code*. The term is used in section 123.1 (Injunctions).

1340. The term means the *Regulatory Powers (Standard Provisions) Act 2014*.

Definition of security classified information

1341. This item inserts a new definition of ***security classified information*** for the purposes of Part 5.6 of the *Criminal Code*. Security classified information is a category of ***inherently harmful information***.

1342. The term is defined as meaning information that has a security classification (within the meaning of section 90.5 of the *Criminal Code*). Subsection 90.5(1) provides that ***security classification*** has the meaning prescribed by the regulations.

Definition of security or defence of Australia

1343. This item inserts a new definition of ***security or defence of Australia*** for the purposes of Part 5.6 of the *Criminal Code*.

1344. Information the communication of which would, or could reasonably be expected to, damage the security or defence of Australia is a category of ***inherently harmful information***. The term should take its ordinary and natural meaning, as including security or military defence of Australia. The term is defined as including the operations, capabilities and technologies of, and methods and sources used by, domestic intelligence agencies or foreign intelligence agencies.

1345. Subsection 121.1(2) provides that, to avoid doubt, the term 'communicates' includes 'publish and make available'.

Section 121.2—Definition of proper place of custody

1346. This item inserts a new section 121.2 which provides the definition of the term ***proper place of custody***.

1347. Subsection 121.2 provides that the definition of ***proper place of custody*** has the meaning prescribed in the regulations. The term is used as part of the offence provisions in subsections 122.1(3) and 122.2(3), which provide that it is an offence in certain circumstances for a person to intentionally remove information from a proper place of custody, or to hold information outside a proper place of custody.

1348. 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.

1349. 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.

1350. 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.

1351. 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.

1352. 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.

1353. Subsection 121.2(2) provides that, despite subsection 14(2) of the *Legislation Act 2003*, regulations made for the purposes of subsection (1) may prescribe a matter by applying, adopting or incorporating any matter contained in an instrument or other writing as in force or existing from time to time. The incorporation of the content of the definition by reference to another instrument or document is necessary to enable the definition to incorporate documents setting out Commonwealth protective security policy documents, to ensure alignment between the Commonwealth's protective security police as in force from time-to-time and the scope of the offences.

1354. The Commonwealth *Protective Security Policy Framework* sets out the Commonwealth's protective security policy as in force from time-to-time. Tier 1, 2 and 3 documents comprising the PSPF are available free of charge online. Tier 4 documents that agencies develop to set out agency-specific protective security policies and procedures are available free of charge to all persons in agencies subject to those policies and procedures.

Section 121.3—Evidentiary certificate

1355. This item inserts a new section 121.3 which provides that, for the purposes of a proceeding for an offence against new Division 122 of the *Criminal Code*, the Attorney-General may sign a certificate (an evidentiary certificate) stating either of the following matters in relation to information or a thing identified in the certificate:

- that the information or thing has, or had at a particular time, a security classification, or

- that the information or thing has, or had at a specified time, a specified level of security classification.

1356. An evidentiary certificate signed by the Attorney-General under section 121.3 is *prima facie* evidence of that matter.

1357. Part 5.3 of the Guide to Framing Commonwealth Offences provides that evidentiary certificates should generally only be used to settle formal or technical matters of fact that would be difficult to prove by adducing admissible evidence.

1358. Security classified information is ordinarily clearly labelled as such. The evidentiary certificate framework in new section 121.3 is intended to facilitate the settling the formal question of whether particular information has, or had a particular time, a security classification or a specified level of security classification, in limited cases where a security

classification is not clearly marked on a particular document or piece of information. This may include cases where, for example:

- a person has communicated information orally, and that information is, or was at the relevant time, security classified
- a person has modified a document to remove any labels denoting its security classification
- a person has communicated an excerpt from a security classified document, and that excerpt does not include a label denoting a security classification
- a person has removed security classified information from a database, and the form in which it was removed does not include a label denoting a security classification, or
- the information or document contains paragraph markings that are an abbreviated or shorthand reference to a security classification.

1359. In such cases, it may be difficult to settle the question of whether the particular information has, or had at a particular time, a security classification or a particular level of security classification, by adducing admissible evidence. It would often be necessary to adduce the original document or information from which the information was drawn into evidence. The admission into evidence of additional security classified information may risk compounding the harm to essential public interests by providing the defendant with additional security classified information that they have no need to know, as well as risking the further exposure of that information.

1360. It would often be necessary to put in place additional controls to protect the security classified information, such as those available under the *National Security Information (Criminal and Civil Proceedings) Act 2004*, which may impose additional burdens on the prosecution, defendant and court. In cases where the question of whether the information is, or was at a particular time, security classified information, or had a particular level of security classification, is essentially formal in nature, the use of a *prima facie* evidentiary certificate would facilitate the settling of that question by avoiding the difficulty of adducing additional classified evidence and the resultant imposition of potentially burdensome obligations on the parties and court.

1361. The evidentiary certificate is only *prima facie* evidence of the fact that the information identified in the certificate has a security classification, or had a security classification at a particular time. The use of a *prima facie* evidentiary certificate will allow a defendant to adduce evidence to the contrary, that the information is not security classified, did not have a security classification at the particular time, does not have a particular level of security classification, or did not have a particular level of security classification at the particular time. Therefore, the use of a *prima facie* evidentiary certificate will not prevent a defendant from contesting the question of whether the information in question is, or was, security classified, either in general or to a particular level.

Division 122—Secrecy of information

1362. This item inserts a new Division 122 to the Criminal Code, which contains new general secrecy offences. These offences replace the general secrecy offences contained in Parts VI and VII of the *Crimes Act 1914* with a modernised and more targeted set of offences, directed at protecting the essential public interests of the Commonwealth.

1363. The new general secrecy offences will criminalise the communication of information, dealing with information, the movement of information outside the proper place of custody, or the failure to comply with a direction regarding information, where:

- the information is inherently harmful information, or
- the conduct causes harm to Australia's interests, or
- the conduct will or is likely to cause harm to Australia's interests.

1364. Division 122 also contains an aggravated offence, applying where a person commits an underlying general secrecy offence and one or more aggravating circumstances exist.

1365. Division 122 further contains a set of defences, which operate to ensure that persons are not criminally liable for the communication of information, dealing with information, movement of information outside a proper place of custody, or the failure to comply with a direction regarding information, where:

- the person was exercising a power, or performing a function or duty, in the person's capacity as a Commonwealth officer or a person who is otherwise engaged to perform work for a Commonwealth entity
- the information has already been communicated or made available to the public with the authority of the Commonwealth
- the person's conduct related to the communication of information to a Commonwealth oversight or integrity body, or was for the purpose of such a body exercising a power, or performing a function or duty
- the person communicated the information in accordance with the *Public Interest Disclosure Act 2013*
- the person's conduct related to the communication of information to a court or tribunal
- the person's conduct related to the communication of the information in the public interest and in the person's capacity as a journalist engaged in fair and accurate reporting
- the information has previously been communicated, or made available, to the public (a prior publication) and the person was not involved in the prior publication, or

- the information relates to the person, is communicated with the consent of the person to whom it relates, or is communicated to the person to whom it relates.

1366. The offences in Division 122 must be read in conjunction with the offence-specific defences, which operate to limit the circumstances in which a person may be criminally liable.

Section 122.1—Inherently harmful information

1367. This item inserts a new section 122.1 to the *Criminal Code*, which contains a set of four general secrecy offences relating to:

- the communication of inherently harmful information;
- dealing with inherently harmful information;
- the movement of inherently information outside the proper place of custody; or
- the failure to comply with a direction regarding inherently harmful information.

1368. ***Inherently harmful information*** is defined in section 121.1, and is comprised of five categories of information the unauthorised disclosure of which would, or would be reasonably likely to, harm essential public interests. Accordingly the offences in section 122.1 do not contain harm elements, requiring the prosecution to prove beyond reasonable doubt that the conduct the subject of the alleged offence caused, or was reasonably likely to cause, harm.

Communicating inherently harmful information

1369. Subsection 122.1(1) creates an offence where a person communicates inherently harmful information that was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity.

1370. The offence will carry a maximum penalty of 15 years imprisonment.

1371. Examples of the offence are as follows:

- Example 1: Person A is an employee of a Commonwealth department. Person A access a classified document from the department's information management system and publishes the document on a publicly available website.
- Example 2: Person B is employed by a domestic intelligence agency. Person B makes a copy of a document produced by a foreign intelligence agency from Country F and provided to the domestic intelligence agency through properly authorised information sharing agreements. Person B discloses the copy of the document to a friend who is an academic undertaking research on Country F.

1372. To establish this offence, the prosecution will need to prove beyond reasonable doubt that:

- the person intentionally communicated information
- either:
    - the information was inherently harmful information (other than security classified information) and the person was reckless as to this element, or
    - the information was security classified information
- the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity and the person was reckless as to this element.

1373. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 122.1(1)(a). Under subsection 5.2(1) of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

1374. Recklessness is the fault element for paragraphs 122.1(1)(b) and (c). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and
- a result if he or she is 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 the risk.

1375. Strict liability will apply to paragraph 122.1(1)(b) to the extent that the information is security classified information consistent with subsection 122.1(5).

1376. For paragraph 122.1(1)(a), the prosecution will have to prove beyond a reasonable doubt that the person intentionally communicated information.

1377. The term ‘communicates’ is taken to include references to ‘publishes’ and ‘makes available’, consistent with subsection 121.1(2). It is intended to include imparting or transmitting information by any means. It is not intended to require, as a rule, proof that the information was received by another person, or proof that another person read, heard or viewed the information. A person would communicate information where, for example, a person sends an email containing information, even if the email is not read by another person.

1378. For paragraph 122.1(1)(b), the prosecution will have to prove that the information was inherently harmful information.

1379. If the information is security classified information within paragraph (a) of the definition of inherently harmful information in section 121.1, strict liability will apply consistent with subsection 122.1(5).

1380. Strict liability is set out in section 6.1 of the Criminal Code. The effect of applying strict liability to an element of an offence means that no fault element needs to be proved and the defence of mistake of fact is available.

1381. Applying strict liability to paragraph 122.1(1)(b) of the offence is appropriate because information carrying a security classification are clearly marked with the security classification and any person who has access to security classified information should easily be able to identify as such.

1382. The defence of mistake of fact is set out in section 9.2 of the Criminal Code. The defence provides that a person is not criminally responsible for an offence that includes a physical element to which strict liability applies if:

- at or before the time of the conduct constituting the physical element, the person considered whether or not a fact existed, and is under a mistaken but reasonable belief about those facts, and

- had those facts existed, the conduct would not have constituted an offence.

1383. The defendant bears an evidential burden in relation to this defence. Section 13.3 of the Criminal Code provides that in the case of a standard 'evidential burden' defence, the defendant bears the burden of pointing to evidence that suggests a reasonable possibility that the defence is made out. If this is done, the prosecution must refute the defence beyond reasonable doubt (section 13.1).

1384. This defence would be available if, for example, a defendant had specifically turned his or her mind to whether he or she was dealing with records that had a security classification and had mistakenly, but reasonably, concluded that the records did not have a security classification.

1385. The application of strict liability is appropriate because information or things carrying a security classification are clearly marked with the security classification and any person who has access to security classified information should easily be able to identify as such.

1386. If the information falls into paragraphs (b) to (d) of the definition of inherently harmful information, the prosecution will have to prove that the defendant was reckless as to the fact that the information was inherently harmful information. Therefore, the defendant will have to be aware of a substantial risk that the information is inherently harmful and, having regard to the circumstance known to him or her, it is unjustifiable to take the risk.

1387. For paragraph 122.1(1)(c), the prosecution will have to prove that the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity.

1388. The fault element of recklessness applies to this element. Therefore, the prosecution will be required to prove beyond reasonable doubt that the person was aware of a substantial risk that the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity and having regard to the circumstances known to the person, it was unjustifiable to take the risk.

1389. ***Commonwealth officer*** is defined in section 121.1. ***Commonwealth entity*** is defined in the Dictionary to the Criminal Code, as being the Commonwealth or a Commonwealth authority. A ***Commonwealth authority*** is a body established by or under a law of the Commonwealth, subject to certain exceptions including for a body established under the *Corporations Act 2001*.

1390. The requirement that the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity is intended to limit the scope of the offence to apply only to inherently harmful information that has been made or obtained, in essence, by the Commonwealth in an official capacity.

1391. The application of the offence to 'a person', in combination with the stipulation paragraph 122.2(1)(c) that the information was 'made or obtained by… any other person' in their capacity as a Commonwealth officer or a person engaged to perform work for a Commonwealth entity is intended to ensure that a person may be criminally liable for subsequent communications of the information, for example where:

- the person has received inherently harmful information from a Commonwealth officer, either directly or indirectly, and subsequently communicates it to another person, or

- the person improperly obtains inherently harmful information that was made or obtained by a Commonwealth officer (for example, by stealing a document containing such information, or unlawfully accessing a computer system containing such information) and subsequently communicates it to another person.

1392. Note 1 to subsection 122.1(1) clarifies that exceptions to the offence are set out at section 122.4.

1393. The maximum penalty for the offence in subsection 122.1(1) is 15 years' imprisonment. The commission of this offence would have serious consequences for the security and defence of Australia, or for the flow of information to the Commonwealth in connection with essential public functions. The maximum penalty needs to be adequate to deter and punish a worst case offence, including intentional or corrupt disclosures of inherently harmful information, and disclosures that may irreparably damage the defence or security of Australia for decades.

Other dealings with inherently harmful information

1394. Subsection 122.1(2) creates an offence where a person deals with inherently harmful information (other than by communicating it) and the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity.

1395. The offence will carry a maximum penalty of five years imprisonment.

1396. Examples of the offence are as follows:

- Example 1: Person A is an employee of a Commonwealth department. Person A copies a classified document and conceals it in their bag to take it home. Person A locks the document in a safe inside their house.

- Example 2: Person B is employed by a Commonwealth authority. Person B has access to sensitive information obtained through the exercise of coercive powers by the Commonwealth authority. Person B downloads a large quantity of sensitive information onto a portable device and takes the device home.

1397. To establish this offence, the prosecution will need to prove beyond reasonable doubt that:

- the person intentionally deals with information (other than by communicating it)

- either:

    - the information was inherently harmful information (other than security classified information) and the person was reckless as to this element, or

    - the information was security classified information, and

- the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity and the person was reckless as to this element.

1398. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 122.1(2)(a). Under subsection 5.2(1) of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

1399. Recklessness is the fault element for paragraphs 122.1(2)(b) and (c). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and

- a result if he or she is 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 the risk.

1400. Strict liability will apply to paragraph 122.1(2)(b) to the extent that the information is security classified information consistent with subsection 122.1(5).

1401. For paragraph 122.1(1)(a), the prosecution will have to prove beyond a reasonable doubt that the person intentionally dealt with information, other than by communicating it.

Consistent with subsection 121.1(2), 'communicating' includes 'publishing' and 'making available'

1402. The term ***deal*** is defined for the purposes of Part 5.6 in section 121.1 as having the meaning given by subsection 90.1(1) of the Criminal Code. The definition is intended to ensure that the offence operates to deter the disclosure of inherently harmful information, which would, or would be reasonably likely to, cause harm to the essential public interests of the Commonwealth. For example, the element will be satisfied where:

- a person intentionally obtains or collects information—each of which would be steps towards the disclosure of the information; or

- a person intentionally copies or conceals the information—such conduct would, or would be likely to, facilitate the disclosure of the information (for example, by preventing its discovery or recovery by authorities and thereby enabling its later disclosure).

1403. However, the element will not be satisfied by a person reading, analysing or using the information. The nature of inherently harmful information is that the harm to the essential public interests of the Commonwealth would have, or could be likely to have, crystallised when the information was disclosed. The object of the offence framework, therefore, is to strongly deter the disclosure of inherently harmful information in the first instance. For example, in the circumstance that information about a sensitive ASIO source of information (being information falling within some or all of paragraphs (a), (b) and (c) of the definition of inherently harmful information) were disclosed, ASIO would likely need to assume that the nature of this source was compromised and take appropriate action to protect the source and its operation, crystallising the harm to Australia's essential public interests.

1404. For paragraph 122.1(2)(b), the prosecution will have to prove that the information was inherently harmful information.

1405. If the information is security classified information within paragraph (a) of the definition of inherently harmful information in section 121.1, strict liability will apply consistent with subsection 122.1(5).

1406. Strict liability is set out in section 6.1 of the Criminal Code. The effect of applying strict liability to an element of an offence means that no fault element needs to be proved and the defence of mistake of fact is available.

1407. Applying strict liability to paragraph 122.1(2)(b) is appropriate because information or things carrying a security classification are clearly marked with the security classification and any person who has access to security classified information should easily be able to identify as such.

1408. The defence of mistake of fact is set out in section 9.2 of the Criminal Code. The defence provides that a person is not criminally responsible for an offence that includes a physical element to which strict liability applies if:

- at or before the time of the conduct constituting the physical element, the person considered whether or not a fact existed, and is under a mistaken but reasonable belief about those facts, and

- had those facts existed, the conduct would not have constituted an offence.

1409. The defendant bears an evidential burden in relation to this defence. Section 13.3 of the Criminal Code provides that in the case of a standard 'evidential burden' defence, the defendant bears the burden of pointing to evidence that suggests a reasonable possibility that the defence is made out. If this is done, the prosecution must refute the defence beyond reasonable doubt (section 13.1).

1410. This defence would be available if, for example, a defendant had specifically turned his or her mind to whether he or she was dealing with records that had a security classification and had mistakenly but reasonably concluded that the records did not have a security classification.

1411. The application of strict liability is appropriate because information or things carrying a security classification are clearly marked with the security classification and any person who has access to security classified information should easily be able to identify as such.

1412. If the information falls into paragraphs (b) to (d) of the definition of inherently harmful information, the prosecution will have to prove that the defendant was reckless as to the fact that the information was inherently harmful information. Therefore, the defendant will have to be aware of a substantial risk that the information is inherently harmful and, having regard to the circumstance known to him or her, it is unjustifiable to take the risk.

1413. For paragraph 122.1(2)(c), the prosecution will have to prove that the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity.

1414. The fault element of recklessness applies to this element. Therefore, the prosecution will be required to prove beyond reasonable doubt that the person was aware of a substantial risk that the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity and having regard to the circumstances known to the person, it was unjustifiable to take the risk.

1415. ***Commonwealth officer*** is defined in section 121.1. ***Commonwealth entity*** is defined in the Dictionary to the Criminal Code, as being the Commonwealth or a Commonwealth authority. A ***Commonwealth authority*** is a body established by or under a law of the Commonwealth, subject to certain exceptions including for a body established under the *Corporations Act 2001*.

1416. The requirement that the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity is intended to limit the scope of the offence to apply only to inherently harmful information that has been made or obtained, in essence, by the Commonwealth in an official capacity.

1417. The application of the offence to 'a person', in combination with the stipulation in paragraph 122.1(2)(c) that the information was 'made or obtained by… any other person' in their capacity as a Commonwealth officer or a person engaged to perform work for a Commonwealth entity is intended to ensure that a person may be criminally liable for subsequent communications of the information, for example where:

- the person has received inherently harmful information from a Commonwealth officer, either directly or indirectly, and subsequently communicates it to another person, or

- the person improperly obtains inherently harmful information that was made or obtained by a Commonwealth officer (for example, by stealing a document containing such information, or unlawfully accessing a computer system containing such information) and subsequently communicates it to another person.

1418. The maximum penalty for the offence in subsection 122.1(2) is five years' imprisonment. This is less than the maximum penalty for the offence in subsection 122.1(1), involving the communication of inherently harmful information. The offence in subsection 122.1(2) is intended to capture behaviour prior to the communication of information that will cause harm to Australia's interests, as well as behaviour that creates an unacceptable risk that such will be improperly communicated or obtained. A maximum penalty of five years' imprisonment is appropriate to recognise the serious harm to the defence and security of Australia, and to the ability for the Australian Government to perform essential public functions, that can arise from the improper dealing in inherently harmful information.

Removing inherently harming information from, or holding inherently harmful information outside, a proper place of custody

1419. Subsection 122.1(3) creates an offence where a person removes inherently harmful information from, or holds such information outside, its proper place of custody, where that information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity.

1420. The offence will carry a maximum penalty of five years' imprisonment.

1421. Examples of the offence are as follows:

- Example 1: Person A is an employee of a Commonwealth department. Person A removes a document given to the department by a foreign government in confidence from its proper place of custody at the department and takes it home. Person A is not approved to hold the document at their home. Person A is aware that the foreign government provided the document to the Commonwealth on the condition it be held in confidence, and breaching this provision could negatively impact the Commonwealth's relationship with the foreign government.

- Example 2: Person B is a former employee of a Commonwealth department. While employed by the Commonwealth department, Person B was approved

to hold classified documents, including some reports prepared by intelligence agencies, at home. Following the cessation of Person B's employment by the Commonwealth department, Person B does not return the documents in his or her possession to the department and continues to hold them in their home.

- Example 3: Person C is an employee of a company engaged to design a new, weapon system for the Australian Defence Force. Person C discovers that they have accidentally taken a document containing highly sensitive information concerning the design of the weapon system home from work. Instead of immediately returning the document to its proper place of custody in the office, Person C places the document in their garbage bin at home.

1422. To establish this offence, the prosecution will need to prove beyond reasonable doubt that:

- the person either:
    - intentionally removed information from a proper place of custody for the information, or
    - intentionally held information outside a proper place of custody for the information
- either:
    - the information was inherently harmful information and the person was reckless as to this, or
    - the information was security classified information
- the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity and the person was reckless as to this.

1423. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 122.1(3)(a). Under subsection 5.2(1) of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

1424. Recklessness is the fault element for paragraphs 122.1(3)(b) and (c). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and
- a result if he or she is 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 the risk.

1425. Strict liability will apply to paragraph 122.1(3)(b) to the extent that the information is security classified information consistent with subsection 122.1(5).

1426. For paragraph 122.1(3)(a), the prosecution will have to prove beyond a reasonable doubt that the person intentionally removed information from a proper place of custody for that information, or that the person intentionally held information outside a proper place of custody for that information.

1427. The term ***proper place of custody*** will have the meaning prescribed by the regulations, in accordance with sections 121.1 and 121.2. The concept of a proper place of custody may be defined by reference to different kinds of information. For example, the proper place of custody for information that has a security classification of TOP SECRET may be more stringently defined than the proper place of custody for information that has a security classification of PROTECTED.

1428. The concept of removing information is intended to include the removal of information by any means, and in any form. This includes, for example, removing a document containing information from a secure location within a premises (being a proper place of custody for that information) and taking it to a non-secure location within that same (being a place that is not a proper place of custody for the information). It is also intended to include the removal of information in electronic form, such as uploading an electronic file containing information from a computer on a secure computer network (being a proper place of custody for that information) to a non-secure cloud storage service (being a place that is not a proper place of custody for the information).

1429. For paragraph 122.1(3)(b), the prosecution will have to prove that the information was inherently harmful information.

1430. If the information is security classified information within paragraph (a) of the definition of inherently harmful information in section 121.1, strict liability will apply consistent with subsection 122.1(5).

1431. Strict liability is set out in section 6.1 of the Criminal Code. The effect of applying strict liability to an element of an offence means that no fault element needs to be proved and the defence of mistake of fact is available.

1432. Applying strict liability to paragraph 122.1(3)(b) of the offence is appropriate because information or things carrying a security classification are clearly marked with the security classification and any person who has access to security classified information should easily be able to identify as such.

1433. The defence of mistake of fact is set out in section 9.2 of the Criminal Code. The defence provides that a person is not criminally responsible for an offence that includes a physical element to which strict liability applies if:

- at or before the time of the conduct constituting the physical element, the person considered whether or not a fact existed, and is under a mistaken but reasonable belief about those facts, and

- had those facts existed, the conduct would not have constituted an offence.

1434. The defendant bears an evidential burden in relation to this defence. Section 13.3 of the Criminal Code provides that in the case of a standard 'evidential burden' defence, the defendant bears the burden of pointing to evidence that suggests a reasonable possibility that

the defence is made out. If this is done, the prosecution must refute the defence beyond reasonable doubt (section 13.1).

1435. This defence would be available if, for example, a defendant had specifically turned his or her mind to whether he or she was dealing with records that had a security classification and had mistakenly but reasonably concluded that the records did not have a security classification.

1436. If the information falls into paragraphs (b) to (d) of the definition of inherently harmful information, the prosecution will have to prove that the defendant was reckless as to the fact that the information was inherently harmful information. Therefore, the defendant will have to be aware of a substantial risk that the information is inherently harmful information and, having regard to the circumstance known to him or her, it is unjustifiable to take the risk.

1437. For paragraph 122.1(3)(c), the prosecution will have to prove that the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity.

1438. The fault element of recklessness applies to this element. Therefore, the prosecution will be required to prove beyond reasonable doubt that the person was aware of a substantial risk that the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity and having regard to the circumstances known to the person, it was unjustifiable to take the risk.

1439. ***Commonwealth officer*** is exhaustively defined in section 121.1. ***Commonwealth entity*** is defined in the Dictionary to the *Criminal Code*, as being the Commonwealth or a Commonwealth authority. A ***Commonwealth authority*** is a body established by or under a law of the Commonwealth, subject to certain exceptions including for a body established under the *Corporations Act 2001*. The exclusion of bodies established under this Act is intended to ensure, among other things, parity between Commonwealth Government-owned companies and their private sector competitors.

1440. The requirement that the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity is intended to limit the scope of the offence to apply only to inherently harmful information that has been made or obtained, in essence, by the Commonwealth in an official capacity.

1441. The application of the offence to 'a person', in combination with the stipulation in the third physical element that the information was 'made or obtained by… any other person' in their capacity as a Commonwealth officer or a person engaged to perform work for a Commonwealth entity is intended to ensure that a person may be criminally liable for subsequent communications of the information, for example where:

- the person has received inherently harmful information from a Commonwealth officer, either directly or indirectly, and subsequently communicates it to another person, or

- the person improperly obtains inherently harmful information that was made or obtained by a Commonwealth officer (for example, by stealing a document containing such information, or unlawfully accessing a computer system containing such information) and subsequently communicates it to another person.

1442. The maximum penalty for the offence in subsection 122.1(3) is five years' imprisonment. This is less than the maximum penalty for the offence in subsection 122.1(1), involving the communication of inherently harmful information. The offence in subsection 122.1(3) is intended to capture behaviour prior to the communication of inherently harmful information, as well as behaviour that creates an unacceptable risk that inherently harmful information will be improperly communicated or obtained.

1443. A maximum penalty of five years' imprisonment is appropriate to recognise the serious harm to the defence and security of Australia, and to the ability for the Commonwealth Government to perform essential public functions, that can arise from removing inherently harmful information from, or holding such information outside, its proper place of custody.

Failure to comply with direction regarding inherently harmful information

1444. Subsection 122.1(4) creates an offence where a person is given a lawful direction regarding the retention, use or disposal of inherently harmful information that was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for the Commonwealth, and the person fails to comply with the direction.

1445. The offence will carry a maximum penalty of five years' imprisonment.

1446. An example of the offence is as follows. Person A is employed under the *Members of Parliament (Staff) Act 1984*. Person A is given a document containing an update on an ongoing criminal intelligence investigation by Person B, a senior official of the Australian Criminal Intelligence Commission. The document contains information obtained using the ACIC's coercive examination powers, and from a source. Person B directs Person A to store the document in a safe that only Person A has access to. Person A stores the document in a safe that is accessible by all staff in the office.

1447. To establish this offence, the prosecution will need to prove beyond reasonable doubt that:

- the person was given a direction and the person was reckless as to this element
- the direction was a lawful direction regarding the retention, use or disposal of information and the person was reckless as to this
- the person intentionally failed to comply with the direction

- either:
    - the information was inherently harmful information (other than security classified information) and the person was reckless as to this element, or
    - the information was security classified information
- the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity and the person was reckless as to this element.

1448. Recklessness is the fault element applying to paragraphs 122.1(4)(a), (b), and (e). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and
- a result if he or she is 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 the risk.

1449. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 122.1(4)(c). Under subsection 5.2(1) of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

1450. Recklessness is the fault element for paragraph 122.1(4)(d) to the extent that the information is inherently harmful information other than security classified information. Strict liability will apply to paragraph 122.1(4)(d) to the extent that the information is security classified information consistent with subsection 122.1(5).

1451. For paragraph 122.1(4)(a), the prosecution will have to prove beyond reasonable doubt that the person was given a direction. A direction can be written or oral. Recklessness is the fault element for this element. Therefore, the person will have to be aware of a substantial risk that he or she was given a direction and, having regard to the circumstances known to him or her, it was unjustifiable to take the risk.

1452. For paragraph 122.1(4)(b), the prosecution will have to prove beyond reasonable doubt that the direction was a lawful direction regarding the retention, use or disposal of information. It is intended that the concept of a lawful direction include a direction that is lawful, from a person with the authority to give that direction. It is not intended that there must exist a formal relationship of command or control between the person who gives the direction and the person to whom the direction is given. Examples of a lawful direction would include:

- Example 1: Person A is an APS employee. Person B is an APS employee of the same agency. Person B gives Person A a direction, and has the authority to give that direction.

- Example 2: Person C is subject to an arrangement or agreement with the Commonwealth, or a Commonwealth entity. Person D gives Person C a direction, and has the authority to give that direction in connection with the arrangement or agreement.

- Example 3: Person E gives Person F information. In the course of giving the information to Person F, Person E gives Person F a direction.

1453. For paragraph 122.1(4)(c), the prosecution will have to prove beyond a reasonable doubt that the person failed to comply with the direction. The fault element of intention applies to this element. Therefore, the prosecution will have to prove that the person meant to fail to comply with the direction.

1454. For paragraph 122.1(4)(d), the prosecution will have to prove beyond reasonable doubt that the information was inherently harmful information. If the information is security classified information within paragraph (a) of the definition of inherently harmful information in section 121.1, strict liability will apply consistent with subsection 122.1(5).

1455. Strict liability is set out in section 6.1 of the Criminal Code. The effect of applying strict liability to an element of an offence means that no fault element needs to be proved and the defence of mistake of fact is available.

1456. Applying strict liability to paragraph 122.1(4)(d) of the offence is appropriate because information or things carrying a security classification are clearly marked with the security classification and any person who has access to security classified information should easily be able to identify as such.

1457. The defence of mistake of fact is set out in section 9.2 of the Criminal Code. The defence provides that a person is not criminally responsible for an offence that includes a physical element to which strict liability applies if:

- at or before the time of the conduct constituting the physical element, the person considered whether or not a fact existed, and is under a mistaken but reasonable belief about those facts, and

- had those facts existed, the conduct would not have constituted an offence.

1458. The defendant bears an evidential burden in relation to this defence. Section 13.3 of the Criminal Code provides that in the case of a standard 'evidential burden' defence, the defendant bears the burden of pointing to evidence that suggests a reasonable possibility that the defence is made out. If this is done, the prosecution must refute the defence beyond reasonable doubt (section 13.1).

1459. This defence would be available if, for example, a defendant had specifically turned his or her mind to whether he or she was dealing with records that had a security classification and had mistakenly, but reasonably, concluded that the records did not have a security classification.

1460. If the information falls into paragraphs (b) to (d) of the definition of inherently harmful information, the prosecution will have to prove that the defendant was reckless as to the fact that the information was inherently harmful information. Therefore, the defendant

will have to be aware of a substantial risk that the information is inherently harmful information and, having regard to the circumstance known to him or her, it is unjustifiable to take the risk.

1461. For paragraph 122.1(4)(e), the prosecution will have to prove that the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity.

1462. The fault element of recklessness applies to this element. Therefore, the prosecution will be required to prove beyond reasonable doubt that the person was aware of a substantial risk that the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity and having regard to the circumstances known to the person, it was unjustifiable to take the risk.

1463. ***Commonwealth officer*** is defined in section 121.1. ***Commonwealth entity*** is defined in the Dictionary to the Criminal Code, as being the Commonwealth or a Commonwealth authority. A ***Commonwealth authority*** is a body established by or under a law of the Commonwealth, subject to certain exceptions including for a body established under the *Corporations Act 2001*.

1464. The requirement that the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity is intended to limit the scope of the offence to apply only to inherently harmful information that has been made or obtained, in essence, by the Commonwealth in an official capacity.

1465. The application of the offence to 'a person', in combination with the stipulation in paragraph 122.1(4)(e) that the information was 'made or obtained by… any other person' in their capacity as a Commonwealth officer or a person engaged to perform work for a Commonwealth entity is intended to ensure that a person may be criminally liable for failing to comply with a direction, for example where the person has received inherently harmful information from a Commonwealth officer, either directly or indirectly, has been given a lawful direction regarding the retention, use or disposal of that information, and fails to comply with that direction.

1466. Note 1 to subsection 122.1 clarifies that exceptions to the offence are set out at section 122.4.

1467. The maximum penalty for the offence in subsection 122.1(4) is five years' imprisonment. This is less than the maximum penalty for the offence in subsection 122.1(1), involving the communication of inherently harmful information. The offence in subsection 122.1(4) is intended to capture behaviour prior to the communication of inherently harmful information, as well as behaviour that creates an unacceptable risk that inherently harmful information will be improperly communicated or obtained.

1468. A maximum penalty of five years' imprisonment is appropriate to recognise the serious harm to the defence and security of Australia, and to the ability for the Commonwealth Government to perform essential public functions, that can arise from a person intentionally failing to comply with a lawful direction regarding the retention, use or disposal of inherently harmful information.

Section 122.2—Conduct causing harm to Australia's interests

1469. This item inserts a new section 122.2 to the *Criminal Code*, which contains a set of four general secrecy offences relating to:

- the communication of official information that causes, will cause, or that is likely to cause harm to Australia's interests;
- dealing with official information that causes, will cause, or that is likely to cause harm to Australia's interests;
- the movement of official information that causes, will cause, or that is likely to cause harm to Australia's interests; or
- the failure to comply with a direction regarding official information that causes, will cause, or that is likely to cause harm to Australia's interests.

1470. ***Cause harm to Australia's interests*** is defined in section 121.1. The definition contains an exhaustive list of matters which represent essential national interests. The use of official information to cause harm to these interests is a serious matter which, in certain circumstances set out in section 122.2, should attract criminal liability.

Communication causing harm to Australia's interests

1471. Subsection 122.2(1) creates an offence where a person communicates information, the communication either causes harm to Australia's interests, or will or is likely to cause harm to Australia's interests, and the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity.

1472. The offence will carry a maximum penalty of 15 years imprisonment.

1473. Examples of the offence are as follows:

- Example 1: Person A is an employee of the Australian Federal Police. Person A accesses a document relating to an ongoing investigation into organised criminal activity from the Australian Federal Police's information management system, and provides the document to a member of the organised crime group that is the subject of the investigation. As a result of the disclosure, the organised crime group destroys a range of evidential material, prejudicing the investigation of its criminal activities.
- Example 2: Person C is a lawyer who has been engaged to perform work for a Commonwealth department in connection with the negotiation of a multilateral treaty. Person D is an official of a Country E involved in the negotiation of the same treaty. Person D gives Person C a document containing details of the Country E's negotiating strategy, and requests that Person C keep that document confidential to the Commonwealth Government negotiating team. Person C provides that document to Person F, who is an official of a Country G involved in the negotiation of the same treaty. As a result of the disclosure, Country E limits the amount of information it provides

to the Commonwealth Government in connection with the negotiation of the treaty.

1474. To establish this offence, the prosecution will need to prove beyond reasonable doubt that:

- the person intentionally communicated information
- either:
    - the communication causes harm to Australia's interests and the person was reckless as to this, or
    - the communication will or is likely to cause harm to Australia's interests and the person was reckless as to this
- the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity and the person was reckless as to this element.

1475. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 122.2(1)(a). Under subsection 5.2(1) of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

1476. Recklessness is the fault element for paragraphs 122.2(1)(b) and (c). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and
- a result if he or she is 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 the risk.

1477. For paragraph 122.2(1)(a), the prosecution will have to prove beyond a reasonable doubt that the person intentionally communicated information.

1478. The term 'communicates' is taken to include references to 'publishes' and 'makes available', consistent with subsection 121.1(2). It is intended to include imparting or transmitting information by any means. It is not intended to require, as a rule, proof that the information was received by another person, or proof that another person read, heard or viewed the information. A person would communicate information where, for example, a person sends an email containing information, even if the email is not read by another person.

1479. For paragraph 122.2(1)(b), the prosecution will have to prove beyond reasonable doubt that either:

- the communication causes harm to Australia's interests, or
- the communication will or is likely to cause harm to Australia's interests.

1480. The fault element of recklessness applies to this physical element. Therefore, the prosecution will be required to prove beyond reasonable doubt that:

- the person was aware of a substantial risk that the communication had, would or was likely to cause harm to Australia's interests, and
- having regard to the circumstances known to the person, it was unjustifiable to take the risk.

1481. In Example 1 above, Person A would be aware of a substantial risk that revealing sensitive information about a law enforcement operation to the subject of the investigation would prejudice the investigation of a criminal offence (which falls within paragraph (a) of the definition of ***causes harm to Australia's interests*** in section 121.1) and that it is unjustifiable to take the risk.

1482. For paragraph 122.2(1)(c), the prosecution will have to prove that the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity.

1483. The fault element of recklessness applies to this element. Therefore, the prosecution will be required to prove beyond reasonable doubt that the person was aware of a substantial risk that the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity and having regard to the circumstances known to the person, it was unjustifiable to take the risk.

1484. ***Commonwealth officer*** is defined in section 121.1. ***Commonwealth entity*** is defined in the Dictionary to the Criminal Code, as being the Commonwealth or a Commonwealth authority. A ***Commonwealth authority*** is a body established by or under a law of the Commonwealth, subject to certain exceptions including for a body established under the *Corporations Act 2001*.

1485. The requirement that the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity is intended to limit the scope of the offence to apply only to information that has been made or obtained, in essence, by the Commonwealth in an official capacity.

1486. The application of the offence to 'a person', in combination with the stipulation in paragraph 122.2(1)(c) that the information was 'made or obtained by… any other person' in their capacity as a Commonwealth officer or a person engaged to perform work for a Commonwealth entity is intended to ensure that a person may be criminally liable for subsequent communications of the information, for example where:

- the person has received information from a Commonwealth officer, either directly or indirectly, and subsequently communicates it to another person, and that communication causes, or will or is likely to cause, harm to Australia's interests, or
- the person improperly obtains information that was made or obtained by a Commonwealth officer (for example, by stealing a document containing such

information, or unlawfully accessing a computer system containing such information) and subsequently communicates it to another person, and that communication causes, or will or is likely to cause, harm to Australia's interests.

1487. Note 1 to subsection 122.2(1) clarifies that the definition of ***causes harm to Australia's interests*** is contained in section 121.1.

1488. Note 2 to subsection 122.2(1) clarifies that exceptions to the offence are set out at section 122.5.

1489. The maximum penalty for the offence in subsection 122.2(1) is 15 years' imprisonment. The commission of this offence would have serious consequences for the essential public interests of Commonwealth. The maximum penalty needs to be adequate to deter and punish a worst case offence, including the communication of official information with the intent of compromising a major law enforcement or national security investigation, or that results in the death of, or serious injury to, a large number of people.

Other conduct causing harm to Australia's interests

1490. Subsection 122.2(2) creates an offence where a person deals with information (other than by communicating it), the dealing causes harm to Australia's interests, or will or is likely to cause harm to Australia's interests, and the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity.

1491. The offence will carry a maximum penalty of five years imprisonment.

1492. Examples of the offence are as follows:

- Example 1: Person A is an employee of the Department of Foreign Affairs and Trade. Person A copies a document given to the department by a foreign government in confidence, conceals it in their bag and takes it to a café. Person A is observed reading the document in the café. The foreign government becomes aware that the document has been copied and removed from the department, and limits the volume of information it shares with the Australian Government in confidence.

- Example 2: Person B is a member of an organised criminal group. Person B convinces Person C, a member of the Australian Federal Police, to disclose information to Person B concerning the planned execution of search warrants over premises relating to Person B's organised criminal activities. Person B then obtains or collects the information from Person C.

1493. To establish this offence, the prosecution will need to prove beyond reasonable doubt that:

- the person intentionally deals with information (other than by communicating it)

- either:
    - the dealing causes harm to Australia's interests and the person was reckless as to this, or
    - the dealing will or is likely to cause harm to Australia's interests and the person was reckless as to this
- the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity and the person was reckless as to this element.

1494. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 122.2(2)(a). Under subsection 5.2(1) of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

1495. Recklessness is the fault element for paragraphs 122.2(2)(b) and (c). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and
- a result if he or she is 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 the risk.

1496. For paragraph 122.2(1)(a), the prosecution will have to prove beyond a reasonable doubt that the person intentionally dealt with information, other than by communicating it. Consistent with subsection 121.1(2), 'communicating' includes 'publishing' and 'making available'

1497. The term ***deal*** is defined for the purposes of Part 5.6 in section 121.1 as having the meaning given by subsection 90.1(1) of the Criminal Code. The definition is intended to ensure that the offence operates to deter the disclosure of inherently harmful information, which would, or would be reasonably likely to, cause harm to the essential public interests of the Commonwealth. For example, the element will be satisfied where:

- a person intentionally obtains or collects information—each of which may either be steps towards the disclosure of the information, or the result of the disclosure of the information, or
- a person intentionally copies or conceals the information—such conduct would, or would be likely to, facilitate the disclosure of the information (for example, by preventing its discovery or recovery by authorities).

1498. However, the element will not be satisfied by a person reading, analysing or using the information. The nature of information that will or is likely to harm Australia's interests is that the harm to those interests would have, or could be likely to have, crystallised when the

information was disclosed. The object of the offence framework, therefore, is to strongly deter the disclosure of such information in the first instance.

1499. For paragraph 122.2(2)(b), the prosecution will have to prove beyond reasonable doubt that either:

- the dealing caused harm to Australia's interests, or
- the dealing was or was likely to cause harm to Australia's interests.

1500. The fault element of recklessness applies to this physical element. Therefore, the prosecution will be required to prove beyond reasonable doubt that:

- the person was aware of a substantial risk that the dealing would or was likely to cause harm to Australia's interests, and
- having regard to the circumstances known to the person, it was unjustifiable to take the risk.

1501. In Example 1 above, Person A would be aware of a substantial risk that copying a document provided by the government of a foreign country and reading it in a public location was likely to harm or prejudice Australia's international relations with the foreign country (which falls within subparagraph (c)(i) of the definition of ***causes harm to Australia's interests*** in section 121.1).

1502. For paragraph 122.2(2)(c), the prosecution will have to prove that the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity.

1503. The fault element of recklessness applies to this element. Therefore, the prosecution will be required to prove beyond reasonable doubt that the person was aware of a substantial risk that the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity and having regard to the circumstances known to the person, it was unjustifiable to take the risk.

1504. ***Commonwealth officer*** is defined in section 121.1. ***Commonwealth entity*** is defined in the Dictionary to the Criminal Code, as being the Commonwealth or a Commonwealth authority. A ***Commonwealth authority*** is a body established by or under a law of the Commonwealth, subject to certain exceptions including for a body established under the *Corporations Act 2001*.

1505. The requirement that the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity is intended to limit the scope of the offence to apply only to inherently harmful information that has been made or obtained, in essence, by the Commonwealth in an official capacity.

1506. The application of the offence to 'a person', in combination with the stipulation in paragraph 122.2(2)(c) that the information was 'made or obtained by… any other person' in their capacity as a Commonwealth officer or a person engaged to perform work for a

Commonwealth entity is intended to ensure that a person may be criminally liable for subsequent dealings with the information, for example where:

- the person has obtained or collected information from a Commonwealth officer, either directly or indirectly, and subsequently conceals the information, preventing its discovery or recovery it to another person; or

- the person improperly obtains information that was made or obtained by a Commonwealth officer (for example, by stealing a document containing such information, or unlawfully accessing a computer system containing such information) and subsequently copies that information.

1507. The maximum penalty for the offence in subsection 122.2(2) is five years' imprisonment. This is less than the maximum penalty for the offence in subsection 122.2(1), relating to the communication of information. The offence in subsection 122.2(2) is intended to capture behaviour prior to the communication of information that will cause harm to Australia's interests, as well as behaviour that creates an unacceptable risk that such information will be improperly communicated or obtained.

1508. A maximum penalty of five years' imprisonment is appropriate to recognise the serious harm to essential public interests, including the compromise of major law enforcement or national security investigations, or the death of, or serious injury to, a large number of people that can arise from a person improperly dealing with such information.

Removing information from, or holding information outside, a proper place of custody

1509. Subsection 122.2(3) creates an offence where a person removes information from, or holds such information outside, its proper place of custody, and that removal or holding causes, or will or is likely to cause, harm to Australia's interests where that information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity.

1510. The offence will carry a maximum penalty of five years' imprisonment.

1511. Examples of the offence are as follows:

- Example 1: Person A is an employee of a Commonwealth department. Person A removes a document given to the department by a foreign government in confidence from its proper place of custody at the department and takes it home. Person A is not approved to hold the document at their home. The foreign government becomes aware that the document has been improperly removed from the department, and limits the volume of information it shares with the Commonwealth Government in confidence.

- Example 2: Person B is an employee of a Commonwealth department. Person B downloads a sensitive briefing for the upcoming Council of Australian Governments meeting which contains detailed analysis about the Commonwealth's negotiating strategy and its views on State and Territory government proposals. Person B uploads that information to a commercial cloud storage service.

1512. To establish this offence, the prosecution will need to prove beyond reasonable doubt that:

- the person either:
    - intentionally removed information from a proper place of custody for the information, or
    - intentionally held information outside a proper place of custody for the information
- either:
    - the removal or holding caused harm to Australia's interests and the person was reckless as to this, or
    - the removal or holding would or was likely to cause harm to Australia's interests and the person was reckless as to this
- the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity and the person was reckless as to this element.

1513. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 122.2(3)(a). Under subsection 5.2(1) of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

1514. Recklessness is the fault element for paragraphs 122.2(3)(b) and (c). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and
- a result if he or she is 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 the risk.

1515. For paragraph 122.2(3)(a), the prosecution will have to prove beyond a reasonable doubt that the person intentionally removed information from a proper place of custody for that information, or that the person intentionally held information outside a proper place of custody for that information..

1516. The term ***proper place of custody*** will have the meaning prescribed by the regulations, in accordance with sections 121.1 and 121.2. The concept of a proper place of custody may be defined by reference to different kinds of information. For example, the proper place of custody for information that has a security classification of TOP SECRET may be more stringently defined than the proper place of custody for information that has a security classification of PROTECTED. It is intended that not all kinds of information may have a proper place of custody. If the regulations do not prescribe a proper place of custody

for a particular kind of information, then a person cannot commit the offence in respect of that kind of information.

1517. The concept of removing information is intended to include the removal of information by any means, and in any form. This includes, for example, removing a document containing information from a secure location within a premises (being a proper place of custody for that information) and taking it to a non-secure location within that same premises (being a place that is not a proper place of custody for the information). It is also intended to include the removal of information in electronic form, such as uploading an electronic file containing information from a computer on a secure computer network (being a proper place of custody for that information) to a non-secure cloud storage service (being a place that is not a proper place of custody for the information).

1518. The concept of holding information, when used as part of the concept of holding information outside a proper place of custody for that information, is broader than the concept of merely retaining information. Holding information is intended to include conduct by which a person keeps information in his or her possession or control. Holding information is also intended to include conduct by which a person prevents or keeps information from being returned to a proper place of custody for that information.

1519. For paragraph 122.2(3)(b), the prosecution will have to prove beyond reasonable doubt that either:

- the removal or holding caused harm to Australia's interests, or
- the removal or holding would or was likely to cause harm to Australia's interests.

1520. The fault element of recklessness applies to this physical element. Therefore, the prosecution will be required to prove beyond reasonable doubt that:

- the person was aware of a substantial risk that the removal or holding would or was likely to cause harm to Australia's interests ; and
- having regard to the circumstances known to the person, it was unjustifiable to take the risk.

1521. In Example 2, Person B would be aware of a substantial risk that his or her dealing with the sensitive briefing would harm or prejudice relations between the Commonwealth and a State or Territory (which falls within paragraph (e) of the definition of ***causes harm to Australia's interests*** in section 121.1).

1522. For paragraph 122.2(3)(c), the prosecution will have to prove that the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity.

1523. The fault element of recklessness applies to this element. Therefore, the prosecution will be required to prove beyond reasonable doubt that the person was aware of a substantial risk that the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work

for a Commonwealth entity and having regard to the circumstances known to the person, it was unjustifiable to take the risk.

1524. ***Commonwealth officer*** is defined in section 121.1. ***Commonwealth entity*** is defined in the Dictionary to the Criminal Code, as being the Commonwealth or a Commonwealth authority. A ***Commonwealth authority*** is a body established by or under a law of the Commonwealth, subject to certain exceptions including for a body established under the *Corporations Act 2001*.

1525. The requirement that the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity is intended to limit the scope of the offence to apply only to inherently harmful information that has been made or obtained, in essence, by the Commonwealth in an official capacity.

1526. The application of the offence to 'a person', in combination with the stipulation in paragraph 122.2(3)(c) that the information was 'made or obtained by… any other person' in their capacity as a Commonwealth officer or a person engaged to perform work for a Commonwealth entity is intended to ensure that a person may be criminally liable for subsequent dealings with the information, for example where:

- the person has obtained or collected information from a Commonwealth officer, either directly or indirectly, and subsequently conceals the information, preventing its discovery or recovery it to another person; or

- the person improperly obtains information that was made or obtained by a Commonwealth officer (for example, by stealing a document containing such information, or unlawfully accessing a computer system containing such information) and subsequently copies that information.

1527. The maximum penalty for the offence in subsection 122.2(3) is 5 years' imprisonment. This is less than the maximum penalty for the offence in subsection 122.2(1), relating to the communication of information. The offence in subsection 122.2(3) is intended to capture behaviour prior to the communication of information that will cause harm to Australia's interests, as well as behaviour that creates an unacceptable risk that such information will be improperly communicated or obtained.

1528. A maximum penalty of five years' imprisonment is appropriate to recognise the serious harm to essential public interests, including the compromise of major law enforcement or national security investigations, or the death of, or serious injury to, a large number of people that can arise from a person removing such information from, or holding such information outside, its proper place of custody.

Failure to comply with direction regarding information

1529. Subsection 122.2(4) creates an offence where a person is given a lawful direction regarding the retention, use or disposal of information that was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for the Commonwealth, the person fails to comply with the direction, and the failure to comply causes, or will or is likely to cause, harm to Australia's interests.

1530. The offence will carry a maximum penalty of five years' imprisonment.

1531. Examples of the offence are as follows:

- Example 1: Person A is employed by a Commonwealth department, and is involved in the negotiation of an international treaty. Person A is travelling internationally for the purposes of the treaty negotiations. Person B is the information technology security adviser for the department. Person B directs Person A to not take any information concerning the negotiation with him or her on the trip in electronic form, due to the risk of Person A's electronic devices being accessed by the intelligence services of the foreign country. Person A fails to comply with this direction and takes information concerning the negotiation with him or her on the trip in electronic form. This information is obtained by the intelligence services of the foreign state, compromising Australia's negotiating position in the treaty negotiations.

- Example 2: Person C is an information technology contractor engaged by a Commonwealth department to develop a new case management system for domestic violence orders. Person D is employed by the Commonwealth department and is responsible for the project. Person D gives Person C a sample of real case files to validate the operation of the system and directs Person C to put in place information security measures to ensure the case files are securely retained. Person D fails to comply with the direction, resulting in information about persons subject to domestic violence order, including their home address and contact details, becoming available on the internet.

1532. To establish this offence, the prosecution will need to prove beyond reasonable doubt that:

- the person was given a direction and the person was reckless as to this element
- the direction was a lawful direction regarding the retention, use or disposal of information and the person was reckless as to this element
- the person intentionally failed to comply with the direction
- either:
    - the failure to comply caused harm to Australia's interests and the person was reckless as to this, or
    - the failure to comply would or was likely to cause harm to Australia's interests and the person was reckless as to this
- the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity and the person was reckless as to this element.

1533. Recklessness is the fault element for paragraphs 122.2(4)(a), (b), (d) and (e). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and

- a result if he or she is 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 the risk.

1534. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 122.1(4)(c). Under subsection 5.2(1) of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

1535. For paragraph 122.2(4)(a), the prosecution will have to prove beyond reasonable doubt that the person was given a direction. A direction can be written or oral. Recklessness is the fault element for this element. Therefore, the person will have to be aware of a substantial risk that he or she was given a direction and, having regard to the circumstances known to him or her, it was unjustifiable to take the risk.

1536. For paragraph 122.2(4)(b), the prosecution will have to prove beyond reasonable doubt that the direction was a lawful direction regarding the retention, use or disposal of information. It is intended that the concept of a lawful direction include a direction that is lawful, from a person with the authority to give that direction. It is not intended that there must exist a formal relationship of command or control between the person who gives the direction and the person to whom the direction is given. Examples of a lawful direction would include:

- Example 1: Person A is an APS employee. Person B is an APS employee of the same agency. Person B gives Person A a direction, and has the authority to give that direction.

- Example 2: Person C is subject to an arrangement or agreement with the Commonwealth, or a Commonwealth entity. Person D gives Person C a direction, and has the authority to give that direction in connection with the arrangement or agreement.

- Example 3: Person E gives Person F information. In the course of giving the information to Person F, Person E gives Person F a direction.

1537. For paragraph 122.2(4)(c), the prosecution will have to prove beyond a reasonable doubt that the person failed to comply with the direction. The fault element of intention applies to this element. Therefore, the prosecution will have to prove that the person meant to fail to comply with the direction.

1538. For paragraph 122.2(4)(d), the prosecution will have to prove beyond reasonable doubt that either:

- the failure to comply caused harm to Australia's interests, or

- the failure to comply would or was likely to cause harm to Australia's interests.

1539. The fault element of recklessness applies to this physical element. Therefore, the prosecution will be required to prove beyond reasonable doubt that:

- the person was aware of a substantial risk that failing to comply would or was likely to cause harm to Australia's interests ; and

- having regard to the circumstances known to the person, it was unjustifiable to take the risk.

1540. In Example 2, above, Person C would be aware of a substantial risk that failure to comply with the direction could result in harm to the safety of a section of the public, being persons subject to domestic violence orders, which falls within paragraph (f) of the definition of ***cause harm to Australia's interests*** at section 121.1.

1541. For paragraph 122.2(4)(e), the prosecution will have to prove that the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity.

1542. The fault element of recklessness applies to this element. Therefore, the prosecution will be required to prove beyond reasonable doubt that the person was aware of a substantial risk that the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity and having regard to the circumstances known to the person, it was unjustifiable to take the risk.

1543. ***Commonwealth officer*** is defined in section 121.1. ***Commonwealth entity*** is defined in the Dictionary to the Criminal Code, as being the Commonwealth or a Commonwealth authority. A ***Commonwealth authority*** is a body established by or under a law of the Commonwealth, subject to certain exceptions including for a body established under the *Corporations Act 2001*.

1544. The requirement that the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity is intended to limit the scope of the offence to apply only to inherently harmful information that has been made or obtained, in essence, by the Commonwealth in an official capacity.

1545. The application of the offence to 'a person', in combination with the stipulation in paragraph 122.2(4)(e) that the information was 'made or obtained by… any other person' in their capacity as a Commonwealth officer or a person engaged to perform work for a Commonwealth entity is intended to ensure that a person may be criminally liable for failing to comply with a direction, for example where the person has received inherently harmful information from a Commonwealth officer, either directly or indirectly, has been given a lawful direction regarding the retention, use or disposal of that information, and fails to comply with that direction.

1546. The maximum penalty for the offence in subsection 122.2(4) is five years' imprisonment. This is less than the maximum penalty for the offence in subsection 122.2(1),

relating to the communication of information. The offence in subsection 122.2(4) is intended to capture behaviour prior to the communication of information that will cause harm to Australia's interests, as well as behaviour that creates an unacceptable risk that such information will be improperly communicated or obtained.

1547. A maximum penalty of five years' imprisonment is appropriate to recognise the serious harm to essential public interests, including the compromise of major law enforcement or national security investigations, or the death of, or serious injury to, a large number of people that can arise from a person failing to comply with a lawful direction regarding the retention, use or disposal of such information

Section 122.3—Aggravated offence

1548. Section 122.3 creates an aggravated offence where a person commits an underlying offence against section 122.1 or 122.2 and one of the following circumstances exist in relation to the commission of the underlying offence:

- the information in relation to which the underlying offence is committed has a security classification of secret or above
- if the commission of the underlying offence involves a record containing the relevant information—the record is marked with a code word, 'for Australian eyes only' or as prescribed by the regulations
- the commission of the underlying offence involves five or more records each of which has a security classification
- the commission of the underlying offence involves the person altering a record to remove or conceal its security classification, or
- at the time the person committed the underlying offence, the person held an Australian Government security clearance.

1549. The aggravated offence will be punishable by a maximum penalty of:

- 20 years' imprisonment, if the maximum penalty for the underlying offence is 15 years' imprisonment, or
- 10 years' imprisonment if the maximum penalty for the underlying offence is five years' imprisonment.

1550. An example of this offence is as follows. Person A is employed as an IT systems administrator at a Commonwealth Government intelligence agency. In this role, Person A had access a large volume of highly classified information and throughout his employment Person A copied 1000 electronic files from the agency's internal holdings to a personal hard drive. Over 100 of the documents copied have a security classification, including 20 that also bear one or more code words, and one document classified as TOP SECRET. Person A publishes all 1000 documents on the internet.

1551. To establish the aggravated offence the prosecution will first need to prove beyond reasonable doubt that a person commits an underlying offence against section 122.1

(Inherently harmful information) or section 122.2 (Conduct causing harm to Australia's interests).

1552. The prosecution will be required to establish beyond reasonable doubt all of the elements constituting the relevant underlying offence, including any fault elements applicable to that offence. The physical and fault elements constituting an offence against section 122.1 and section 122.2 are described above.

1553. Subsection 122.3(2) provides that there is no fault element for the physical element described in paragraph 122.3(1)(a) other than the fault elements for the underlying offence. The underlying offences themselves have specific physical and fault elements that must be proved by the prosecution. The prosecution will be required to establish beyond reasonable doubt all of the elements constituting the relevant underlying offence, including any fault elements applicable to that offence. Subsection 122.3(2) makes clear that for the purposes of the offence in section 122.3, the prosecution does not need to prove any fault elements in addition to those fault elements already applying to the underlying offences.

1554. In addition to establishing the underlying offence, the prosecution will need to prove at least one of the following additional elements in relation to the commission of the underlying offence beyond reasonable doubt that:

- information in relation to which the underlying offence was committed had a security classification of SECRET or above (subparagraph 122.3(1)(b)(i))
- if the commission of the underlying offence involved a record—the record was marked with a code word, 'for Australian eyes only' or as prescribed by the regulations (subparagraph 122.3(1)(b)(ii))
- the commission of the underlying offence involved five or more records each of which has a security classification (subparagraph 122.3(1)(b)(iii))
- the commission of the underlying offence involved the person altering a record to remove or conceal its security classification (subparagraph 122.3(1)(b)(iv)), or
- that at the time the person committed the underlying offence, the person held an Australian Government security clearance (subparagraph 122.3(1)(b)(v)).

1555. Section 5.6 of the Criminal Code will apply the automatic fault element of recklessness to the circumstances in subparagraphs 122.3(1)(b)(i), (ii), (iv) and (v). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and
- a result if he or she is 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 the risk.

1556. Strict liability applies to the aggravating factor in subparagraph 122.3(1)(b)(iii) that the commission of the underlying offence involved five or more records each of which has a security classification.

1557. For subparagraph 122.3(1)(b)(i), the prosecution will need to prove beyond reasonable doubt that the commission of the underlying offence involved information that had a security classification of secret or above. A security classification of secret or above is intended to refer to a classification in accordance with the Australian Government's Protective Security Policy Framework (PSPF) and represents an assessment that the disclosure of such information would likely cause serious or exceptionally grave damage to Australia's national interest, organisations or individuals.

1558. The *Australian Government Protective Security Governance Guidelines—Business Impact Levels* provide examples of the kinds of damage that would justify a security classification of secret, including:

- where the compromises damages the operational capacity of an agency—the compromise causes a severe degradation in, or loss of, organisational capability to an extent and duration that the agency cannot perform any of its functions

- where the compromise causes damage to the Australian economy—the compromise causes:

    - major, long-term damage to the Australian economy to an estimated total in excess of $20 billion, or

    - major, long-term damage to global trade or commerce, leading to prolonged recession or hyperinflation in Australia

- where the compromise causes damage to Government policies—the compromise:

    - severely disadvantages Australia in major international negotiations or strategy

    - threatens directly the internal stability of Australia or friendly countries leading to widespread instability

    - raises international tension, or causes severe damage or disruption, to diplomatic relations, or

- where the compromise relates to individual safety—the compromise threatens life directly, and could reasonably be expected to lead to loss of life for an individual or small group.

1559. In the example above, Person A copied, removed from its proper place of custody, and published a document classified as TOP SECRET, which would fall within subparagraph 122.3(1)(b)(i).

1560. The prosecution will have to prove that the defendant was reckless as to whether the information has a security classification of secret or above. Therefore, the defendant must

have been aware of a substantial risk that the information has a security classification of secret or above and, having regard to the circumstances known to him or her, it was unjustifiable to take that risk.

1561. For subparagraph 122.3(1)(b)(ii), the prosecution will have to prove beyond reasonable doubt that the commission of the underlying offence involved a record containing information that is marked with a code word, the phrase "for Australian eyes only", or as prescribed by the regulations for the purposes of this subparagraph.

1562. The inclusion of a protective marking on a record denotes that the record contains information that requires special protection or handling, beyond that which would ordinarily be required based on the record's security classification. The unauthorised disclosure of, or improper dealing with, such information is a particularly serious matter justifying a higher maximum penalty, because:

- of the particular harms that are likely to arise, if the information is improperly disclosed or handled, and
- a person who holds a record containing such a marking is on-notice as to the need for special protection for the information contained therein, either because:
    - if the person is familiar with the marking, the nature of the information it protects, and the requirements that apply to it—the person has actual knowledge of those matters; or
    - if the person is unfamiliar with the marking—the person is, or ought reasonably to be, on notice as to the fact that the information contains information of some particular sensitivity, and more importantly, that the person likely cannot accurately predict the harm that would arise should it be improperly disclosed or handled.

1563. 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.

1564. The phrase 'for Australian eyes only' indicates that the information may only be passed to appropriately security cleared Australian citizens (including dual citizens), on a need-to-know basis. Foreign nationals cannot be allowed access to such information, even if they hold an appropriate Australian security clearance.

1565. 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.

1566. In the example above, Person A copied, removed from its proper place of custody, and published 20 records marked with one or more code words, which would fall within subparagraph 122.3(1)(b)(ii).

1567. The prosecution will have to prove that the defendant was reckless as to whether the record was marked with a code word, 'for Australian eyes only' or as prescribed by the regulations. Therefore, the defendant must have been aware of a substantial risk that the record was marked with a code word, 'for Australian eyes only' or as prescribed by the regulations and, having regard to the circumstances known to him or her, it was unjustifiable to take that risk.

1568. For subparagraph 122.3(1)(b)(iii), the prosecution will need to prove beyond reasonable doubt that the defendant dealt with five or more records or articles, each of which has a security classification, in relation to the commission of the underlying offence. ***Security classification*** is defined in section 90.5, to be inserted by Item 16 of Schedule 1.

1569. In accordance with subsection 122.3(3), strict liability applies to this subparagraph. Strict liability is set out in section 6.1 of the Criminal Code. The effect of applying strict liability to an element of an offence means that no fault element needs to be proved and the defence of mistake of fact is available.

1570. Applying strict liability to subparagraph 122.3(1)(b)(iii) of the offence is appropriate because information or things carrying a security classification are clearly marked with the security classification and any person who has access to security classified information

should easily be able to identify as such. It is not appropriate for a person to be able to avoid criminal responsibility for the aggravating factor at subparagraph 122.3(1)(b)(iii) by claiming, for example, that they knew they were dealing with three documents with a security classification but not with five.

1571. The defence of mistake of fact is set out in section 9.2 of the Criminal Code. The defence provides that a person is not criminally responsible for an offence that includes a physical element to which strict liability applies if:

- at or before the time of the conduct constituting the physical element, the person considered whether or not a fact existed, and is under a mistaken but reasonable belief about those facts, and
- had those facts existed, the conduct would not have constituted an offence.

1572. The defendant bears an evidential burden in relation to this defence. Section 13.3 of the Criminal Code provides that in the case of a standard 'evidential burden' defence, the defendant bears the burden of pointing to evidence that suggests a reasonable possibility that the defence is made out. If this is done, the prosecution must refute the defence beyond reasonable doubt (section 13.1).

1573. This defence would be available if, for example, a defendant had specifically turned his or her mind to whether he or she was dealing with records that had a security classification and had mistakenly but reasonably concluded that the records did not have a security classification.

1574. In the example above, Person A copied, removed from its proper place of custody, and published 100 records which had a security classification, which would fall within subparagraph 122.3(1)(b)(iii).

1575. For subparagraph 122.3(1)(b)(iv), the prosecution will need to prove beyond reasonable doubt that the defendant altered a record or article to remove or conceal its security classification. ***Security classification*** is defined in section 90.5, to be inserted by Item 16 of Schedule 1.

1576. The terms 'altered', 'conceal' and 'remove' are not defined and are intended to take their ordinary meanings:

- The term *altered* is intended to cover the situation where a person amends or changes information in any way. This includes amending a classified document to change or delete the classification marker or to change specific terms in a document to remove identifying details while retaining the original meaning of the document.
- The term *conceals* is intended to cover hiding or preventing the security classification from being seen.
- The term *remove* is intended to cover erasing or taking away the security classification. This would include editing a document to delete the security classification.

1577. Removing or altering a security classification is an aggravating factor because the government imposes a security classification to a document to specifically denote the sensitivity of the information to Australian Government – and the removal or alteration of a security classification is an overt contravention of this key principle of protective security. Removing or altering security classifications can also help an individual evade detection in the process of removing a document from a secure environment by passing the record off as being unclassified or suitable for removal. A person who takes such active steps to facilitate and conceal the commission of the underlying offence demonstrates a particularly high level of culpability, justifying a higher maximum penalty.

1578. Subparagraph 122.3(1)(b)(iv) provides that an aggravating circumstance is where, at the time the person committed the underlying offence, the person held an Australian Government security clearance. Recklessness applies to this element, therefore the prosecution will need to establish that the defendant was aware of a substantial risk that he or she held an Australian Government security clearance and, having regard to the circumstances known to him or her it was unjustifiable to take that risk.

1579. *Australian Government security clearance* is not defined but is intended to capture security clearances granted by the Australian Government Security Vetting Agency (AGSVA) or another government agency conducting and issuing security clearances under the Protective Security Policy Framework. It would capture, for example, security clearances from Baseline to Top Secret Positive Vetting level.

1580. Subparagraph 91.6(1)(b)(v)is an aggravating factor because people who hold a security clearance will be aware of appropriate information handling practices and the importance of protecting information as part of the an application and screening processes to obtain the security clearance.

1581. The maximum penalty for the aggravated offence depends on the maximum penalty for the underlying offence. If the penalty of the underlying offence is imprisonment for 15 years, which applies to the offences for the communication of inherently harmful information or information causing harm to Australia' interests, the penalty for the aggravated offence is imprisonment for 20 years.

1582. If the penalty for the underlying offence is imprisonment for five years, which is the case for the remaining offences involving other kinds of dealing, moving information from its proper place of custody, or failing to comply with a lawful direction, the penalty for the aggravated offence is imprisonment for 10 years.

1583. The higher maximum penalty reflects the higher level of culpability associated with proof of the circumstances set out in paragraph 122.3(1)(b) and the extreme risk posed to Australia's national security in such cases. The penalties for the aggravated offence are consistent with the established principle of Commonwealth criminal law policy as set out in the Guide to Framing Commonwealth Offences to impose a higher penalty where the consequences of the offence are particularly dangerous or damaging.

1584. Subsection 122.3(4) provides that, to avoid doubt, a person does not commit an underlying offence for the purpose of the first physical element, if the person has a defence to the underlying offence. The subsection also provides that a person may be convicted of the aggravated offence, even if they person has not been convicted of the underlying offence. In

such a case, it would be necessary for the prosecution to prove the commission of the underlying offence.

Section 122.4—Unauthorised disclosure of information by Commonwealth officers and former Commonwealth officers

1585. Subsection 122.4 creates an offence where a person communicates information, the person made or obtained the information by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity, the person is under a duty not to disclose the information, and the duty arises under a law of the Commonwealth.

1586. The offence will carry a maximum penalty of two years' imprisonment.

1587. The offence is a modernised form of the general secrecy offence from section 70 of the Crimes Act, applying to current and former Commonwealth officers who communicate information in breach of a legal duty of non-disclosure arising under a law of the Commonwealth.

1588. At present, many Acts and Regulations impose duties of non-disclosure on Commonwealth officers that enliven the offence in section 70 of the Crimes Act. If section 70 were repealed without replacement, those duties would lose their criminal enforceability, potentially undermining the protection of information that should appropriately be protected.

1589. The offence in section 122.4 is intended to preserve the operation of those specific secrecy 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 will be conducted as each duty is next considered, rather than within a specific period of time. Accordingly, this offence is not subject to a sunset provision.

1590. Examples of the offence are as follows:

- Example 1: Person A is an APS employee and obtains information in connection with his or her employment as an APS employee that was communicated in confidence within the government. Subregulation 2.1(4) of the *Public Service Regulations 1999* provides that the APS employee must not disclose such information. Person A communicates the information otherwise than in accordance with subregulation 2.1(5), which sets out the circumstances in which an APS employee may disclose such information.

- Example 2: Person B is a member of the Australian Federal Police, which is an ***interception agency*** within the meaning of the *Telecommunications (Interception and Access) Act 1979*. Person B receives an interception capability plan, containing the details of a Carrier X's strategies for compliance with its legal obligation to provide interception capabilities in relation to its telecommunications services. Section 202 of the Act provides that Person B, as an employee of an interception agency, must treat the plan as confidential, and ensure that is not disclosed to any person or body who is not listed in section 202 without the written permission of the carrier. Person B

communicates the plan to his or her friend, who owns a carrier that is a competitor of Carrier X.

1591. To establish this offence, the prosecution will need to prove beyond reasonable doubt that:

- the person intentionally communicated information
- the person made or obtained the information by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity and the person was reckless as to this element
- the person was under a duty to not disclose the information and the person is reckless as to this element, and
- the duty arose under a law of the Commonwealth.

1592. Section 5.6 of the Criminal Code will apply the automatic fault element of intention to paragraph 122.4(1)(a). Under subsection 5.2(1) of the Criminal Code, a person has intention with respect to conduct if he or she means to engage in that conduct.

1593. Recklessness is the fault element applying to paragraphs 122.4(1)(b) and (c). Section 5.4 of the Criminal Code provides that a person is reckless with respect to:

- a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk, and
- a result if he or she is 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 the risk.

1594. Absolute liability applies in relation to paragraph 122.4(1)(d), consistent with subsection 122.4(2).

1595. For paragraph 122.4(1)(a), the prosecution will have to prove beyond a reasonable doubt that the person intentionally communicated the information.

1596. The term ‘communicates’ is taken to include references to ‘publishes’ and ‘makes available’, consistent with subsection 121.1(2). It is intended to include imparting or transmitting information by any means. It is not intended to require, as a rule, proof that the information was received by another person, or proof that another person read, heard or viewed the information. A person would communicate information where, for example, a person sends an email containing information, even if the email is not read by another person.

1597. For paragraph 122.4(1)(b), the prosecution will have to prove beyond reasonable doubt that the person made or obtained the information by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity.

1598. The fault element of recklessness applies to this element. As a result, the prosecution will have to prove that the defendant was reckless as to the fact that the person made or

obtained the information by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity. Therefore, the defendant will have to be aware of a substantial risk that he or she made or obtained the information by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity and, having regard to the circumstance known to him or her, it was unjustifiable to take the risk.

1599. ***Commonwealth officer*** is defined in section 121.1. ***Commonwealth entity*** is defined in the Dictionary to the Criminal Code, as being the Commonwealth or a Commonwealth authority. A ***Commonwealth authority*** is a body established by or under a law of the Commonwealth, subject to certain exceptions including for a body established under the *Corporations Act 2001*.

1600. For paragraph 122.4(1)(c), the prosecution will have to prove beyond reasonable doubt that the person was under a duty to not disclose the information.

1601. The fault element of recklessness applies to this element. As a result, the prosecution will have to prove that the defendant was reckless as to the fact that he or she was under a duty to not disclose the information. Therefore, the defendant will have to be aware of a substantial risk that he or she was under a duty to not disclose the information and, having regard to the circumstance known to him or her, it was unjustifiable to take the risk.

1602. For paragraph 122.4(1)(d), the prosecution will have to prove beyond reasonable doubt that the duty referred to in paragraph 122.4(1)(c) arose under a law of the Commonwealth.

1603. Absolute liability applies to this element consistent with subsection 122.4(2). As a result, there is no fault element for this element, and the defence of mistake of fact under section 9.2 is unavailable in relation to this physical element.

1604. It is appropriate to apply absolute liability to these matters because requiring proof of fault of the particular element to which strict or absolute liability applies would undermine deterrence, and there are legitimate grounds for penalising persons lacking 'fault' in respect of this element. This is consistent with Commonwealth criminal law practice, as described in the Guide to Framing Commonwealth Offences.

1605. A person can only be criminally liable for the offence against section 122.4 if they are reckless as to whether they are subject to a duty to not disclose the information in question. The question of whether that duty arises under the law of the Commonwealth is, effectively, a question of law. The general position, set out in sections 9.3 and 9.4 of the Criminal Code, is that a person can be criminally responsible for an offence even if, at the time of the conduct constituting the offence, he or she is mistaken about, or ignorant of, the existence or content of an Act or subordinate legislation. Consistent with those general principles of the criminal law, a person should not be excused from criminal liability where they are reckless as to whether they are subject to a duty of non-disclosure, merely because they are mistaken or ignorant about whether that duty arises under a law of the Commonwealth, or under some other source.

1606. The maximum penalty for the offence in subsection 122.4 is two years' imprisonment. This penalty is consistent with the maximum penalty for the offence currently contained in section 70 of the *Crimes Act 1914*.

Section 122.5—Defences

1607. This item inserts new section 122.5 to the Criminal Code, which contains a suite of offence-specific defences to the offences in sections 122.1, 122.2 and 122.4, and which thereby also operate to limit the circumstances in which a person may be criminally liable for the aggravated offence in section 122.3.

1608. The offences in Division 122 are only intended to apply where a person's dealing with information is not a proper or legitimate part of their work. There are a vast range of legitimate circumstances in which Commonwealth officers, persons engaged to perform work on behalf of a Commonwealth entity, and other persons deal with inherently harmful information, or information the communication of which would cause harm to Australia's interests, in performing their duties. For example, possessing or copying information concerning national security is a day to day occurrence in many Commonwealth departments and agencies, for Ministers and their staff, for State and Territory law enforcement agencies working on counter-terrorism investigations, and for defence contractors. It is not intended to criminalise these dealings.

1609. These offence-specific defences operate to supplement the circumstances set out in Part 2.3 of the Criminal Code in which there is no criminal responsibility.

1610. Both the AFP and the CDPP consider the availability of any defences when considering whether to investigate and prosecute criminal offences. In relation to prosecution decisions, the Prosecution Policy of the Commonwealth specifically requires the CDPP to take into account any lines of defence which are plainly open to, or have been indicated by, the alleged offender in deciding whether there is a reasonable prospect of a conviction being secured.

Powers, functions and duties in a person's capacity as a Commonwealth officer etc. or under arrangement

1611. Subsection 122.5(1) will provide a defence if:

- the person was exercising a power, or performing a function or duty, in the person's capacity as a Commonwealth officer or a person who is otherwise engaged to perform work for a Commonwealth entity.; or

- the person dealt with, removed or held the information in accordance with an arrangement or agreement to which the Commonwealth or a Commonwealth entity is party and which allows for the exchange of information.

1612. Section 10.5 of the Criminal Code provides a general defence of lawful authority applicable to all Commonwealth offences. This defence is narrow and only applies to conduct that is specifically justified or excused by a law. Consistent with the definition of ***law*** in the Dictionary to the Criminal Code, this means the conduct must be specifically justified or excused by a law of the Commonwealth, and includes the Criminal Code.

1613. The defence at paragraph 122.5(1)(a) is broader than the lawful authority defence available under section 10.5, and will cover a person was exercising a power, or performing a function or duty, in the person's capacity as a Commonwealth officer or a person who is

otherwise engaged to perform work for a Commonwealth entity, rather than the law of the Commonwealth needing to specifically justify or excuse the person's conduct.

1614. It is intended that the defence in paragraph 122.5(1)(a) should allow for the exercise of professional judgment and the taking of appropriate risks, recognise that in certain circumstances it is necessary to risk or cause a lesser harm to avert a greater harm, and recognise that in certain circumstances decisions made in a person's capacity as a Commonwealth officer or a person who is otherwise engaged to perform work for a Commonwealth entity may cause harm to Australia's interests. For example, a member of the AFP should not be criminally liable if they make a reasonable operational judgment to communicate criminal intelligence to a potential witness, which may risk prejudicing an investigation, in an attempt to elicit important evidence from that witness. Similarly, the Minister or senior official should not be criminally liable if they include a statement of government policy concerning a matter of international significance in official remarks, and a foreign government takes umbrage at the Australian Government's policy on that matter resulting to harm to Australia's international relations with that foreign government.

1615. The defence at paragraph 122.5(1)(b) applies when person dealt with, removed or held the information in accordance with an agreement or arrangement to which the Commonwealth or a Commonwealth entity is party allowing for the exchange of information. Many departments and agencies share information with State, Territory and international counterparts, private companies, and individuals as part of their normal business dealings. Often this information is highly sensitive and highly classified. This defence provides that the secrecy offences in Division 122 do not apply if a person's conduct was in accordance with an agreement or arrangement to which the Commonwealth or a Commonwealth entity was a party and which allows for the exchange of information.

1616. The terms 'arrangement' and 'agreement' are not defined and will be given their ordinary meaning. The term 'agreement' is not intended to be limited by the meaning of 'agreement' in Australian international practice as being a treaty, nor is it intended to require evidence of a formal contractual or legal agreement. It is intended that such terms will capture agreements or arrangements in a range of forms, including those made by exchange of letters or as a memorandum of understanding. It is also intended that such terms will include *ad hoc* agreements or arrangements, including non-disclosure agreements relating to discrete pieces of information.

1617. The Note under the defence at subsection 122.5(1) clarifies that the defendant will bear an evidential burden in relation to this defence. Section 13.3 of the Criminal Code provides that in the case of a standard 'evidential burden' defence, the defendant bears the burden of pointing to evidence that suggests a reasonable possibility that the defence is made out. If this is done, the prosecution must refute the defence beyond reasonable doubt (section 13.1). The imposition of the evidential burden on the defendant 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 official or a person engaged to perform work for a Commonwealth entity, or was in accordance with an information exchange agreement or arrangement.

Information that is already public

1618. Subsection 122.5(2) will provide a defence if the information in relation to which the offence is committed is information that has already been communicated or made available to the public with the authority of the Commonwealth.

1619. It is intended that, where the Commonwealth has made inherently harmful information or information that would cause harm to Australia's interests public, that persons should be free to deal in that information.

1620. It is intended that communicating or making available information to 'the public' includes to the public at large, to a segment of the public, or to individual members of the public or a segment of the public on request. Information can be made available to the public, even if no member of the public actually obtains or collects the information. For example, it is intended that:

- information will be communicated to the public if it is included in a speech or interview given in public or to a professional forum;
- information will be made available to the public if it is posted on a publicly-accessible website, even if no one visits the website; and
- information will be made available to the public if members of the public are entitled to request access to the information, even if no members of the category do request access to it.

1621. Comparatively, it is intended that information will not be communicated or made available to the public if the information is communicated or made available to persons subject to a confidentiality or non-disclosure agreement, or on the expectation of confidentiality.

1622. It is intended that information will be made available 'with the authority of the Commonwealth' if it is made available with the authority of a Commonwealth officer or a person otherwise engaged to perform work for the Commonwealth who has the authority to make the information public.

1623. The Note under the defence at subsection 122.5(2) clarifies that the defendant will bear an evidential burden in relation to this defence. Section 13.3 of the Criminal Code provides that in the case of a standard 'evidential burden' defence, the defendant bears the burden of pointing to evidence that suggests a reasonable possibility that the defence is made out. If this is done, the prosecution must refute the defence beyond reasonable doubt (section 13.1). The imposition of the evidential burden on the defendant is appropriate because the defendant should be readily able to point to evidence that the information was publicly available, and to found a suggestion of a reasonable possibility that the information was communicated or made public with the authority of the Commonwealth.

Information communicated to the Inspector-General of Intelligence and Security, the Commonwealth Ombudsman or the Law Enforcement Integrity Commissioner

1624. Subsection 122.5(3) will provide a defence to a prosecution relating to the communication of information under Division 122 if the person communicated the information:

- to the Inspector-General of Intelligence and Security, the Commonwealth Ombudsman, or the Law Enforcement Integrity Commissioner, or to their staff; or

- for the purpose of the Inspector-General, the Ombudsman or the Commissioner exercising a power, or performing a function or duty.

1625. It is intended that the general secrecy offences should in no way impinge on the ability of the Inspector-General, the Ombudsman, or the Integrity Commissioner, or their staff, to exercise their powers, or to perform their functions or duties. These officials are typically entitled to access any information in the course of performing their functions and duties, reflecting the paramount importance of effective oversight of the intelligence community, law enforcement agencies and the public service.

1626. It is intended that the defence in subsection 122.5(3) be available for a prosecution for dealing with information, moving information from its proper place of custody, or failing to comply with a direction if the person's conduct 'related to' the communication of information to an oversight body, or for the purposes of an oversight body. For example, it is intended that a person be permitted to copy a document for the purpose of communicating the copy to an oversight body. Similarly, in the course of communicating information to an oversight body, it may be necessary for the person to temporarily remove the information from its proper place of custody or to breach a direction regarding the retention of that information (such as a direction that the information not be removed from a particular place). However, it is not intended that a person should be able to continue dealing in or holding information, if they have no intention of actually communicating it to an oversight body, or have ceased to have that intention.

1627. The Note under the defence at subsection 122.5(3) clarifies that the defendant will bear an evidential burden in relation to this defence. Section 13.3 of the Criminal Code provides that in the case of a standard 'evidential burden' defence, the defendant bears the burden of pointing to evidence that suggests a reasonable possibility that the defence is made out. If this is done, the prosecution must refute the defence beyond reasonable doubt (section 13.1). The imposition of the evidential burden on the defendant for the purposes of paragraph 122.5 (3)(a) is appropriate because the defendant should be readily able to point to evidence founding a suggestion that there is a reasonable possibility that their conduct related to the communication of the information to an oversight body. Additionally, requiring the prosecution to prove beyond reasonable doubt that a person's conduct was not for such a purpose would often prove an insurmountable barrier to a successful prosecution, undermining the deterrent effect of the new general secrecy offences.

1628. The imposition of the evidential burden on the defendant for the purposes of paragraph 122.5(3)(b) is appropriate because the person should be readily able to point to evidence that there is a reasonable possibility that their conduct related to providing the

information an oversight agency for the purpose of that agency exercising a power or performing a function or duty.

Information communicated in accordance with the Public Interest Disclosure Act 2013

1629. Subsection 122.5(4) will provide a defence to a prosecution for an offence relating to the communication of information, if the person communicated the information in accordance with the *Public Interest Disclosure Act 2013*. The PID Act establishes a legislative scheme to investigate allegations of wrongdoing in the Commonwealth public sector and provide robust protections for current or former public officials who make qualifying public interest disclosures under the scheme. The scheme covers persons in, or with a relevant connection to, the Commonwealth public sector and includes directors and officers of bodies subject to the *Commonwealth Authorities and Companies Act 1997* as well as employees of Commonwealth intelligence agencies and law enforcement agencies and, in certain circumstances contractors providing services to the Commonwealth as well as their employees.

1630. It is intended that the general secrecy offences should in no way impinge on the operation of the PID Act.

1631. It is intended that the defence in subsection 122.5(4) be available for a prosecution for dealing with information, moving information from its proper place of custody, or failing to comply with a direction if the person's conduct 'related to' the communication of information to in accordance with the PID Act. For example, it is intended that a person be permitted to copy a document for the purpose of communicating the copy in accordance with the PID Act. Similarly, in the course of communicating information in accordance with the PID Act, it may be necessary for the person to temporarily remove the information from its proper place of custody or to breach a direction regarding the retention of that information (such as a direction that the information not be removed from a particular place), in particular if the person makes an external disclosure in accordance with the PID Act. However, it is not intended that a person should be able to continue dealing in or holding information, if they have no intention of actually communicating it in accordance with the PID Act, or have ceased to have that intention.

1632. The Note under the defence at subsection 122.5(4) clarifies that the defendant will bear an evidential burden in relation to this defence. Section 13.3 of the Criminal Code provides that in the case of a standard 'evidential burden' defence, the defendant bears the burden of pointing to evidence that suggests a reasonable possibility that the defence is made out. If this is done, the prosecution must refute the defence beyond reasonable doubt (section 13.1). The imposition of the evidential burden on the defendant is appropriate because the defendant should be readily able to point to evidence that there is a reasonable possibility that their conduct related to the communication of the information in accordance with the PID Act. Additionally, requiring the prosecution to prove beyond reasonable doubt that a person's conduct was not for such a purpose would often prove an insurmountable barrier to a successful prosecution, undermining the deterrent effect of the new general secrecy offences.

Information communicated to a court or tribunal

1633. Subsection 122.5(5) will provide a defence to a prosecution for an offence relating to the communication of information, if the person communicated the information to a court or tribunal (whether or not as a result of a requirement).

1634. It is intended that the general secrecy offences should in no way impinge on the ability for courts to receive information, reflecting the public interest in the full availability of relevant information in the administration of justice. Similarly, it is intended that the general secrecy offences should in no way impinge on the ability for tribunals to receive information, reflecting the necessity for tribunals reviewing administrative decisions to have access to full information to make the most appropriate decisions.

1635. It is intended that the defence in subsection 122.5(5) be available for a prosecution for dealing with information, moving information from its proper place of custody, or failing to comply with a direction if the person's conduct 'related to' the communication of information to a court or tribunal. For example, it is intended that a person be permitted to copy a document for the purpose of communicating the copy to a court or tribunal. Similarly, in the course of communicating information to a court or tribunal, it may be necessary for the person to temporarily remove the information from its proper place of custody or to breach a direction regarding the retention of that information (such as a direction that the information not be removed from a particular place). However, it is not intended that a person should be able to continue dealing in or holding information, if they have no intention of actually communicating it to a court or tribunal, or have ceased to have that intention.

1636. The Note under the defence at subsection 122.5(5) clarifies that the defendant will bear an evidential burden in relation to this defence. Section 13.3 of the Criminal Code provides that in the case of a standard 'evidential burden' defence, the defendant bears the burden of pointing to evidence that suggests a reasonable possibility that the defence is made out. If this is done, the prosecution must refute the defence beyond reasonable doubt (section 13.1). The imposition of the evidential burden on the defendant is appropriate because the defendant should be readily able to point to evidence that there is a reasonable possibility that their conduct related to the communication of the information to a court or tribunal. Additionally, requiring the prosecution to prove beyond reasonable doubt that a person's conduct was not for such a purpose would often prove an insurmountable barrier to a successful prosecution, undermining the deterrent effect of the new general secrecy offences.

Information dealt with or held for the purposes of fair and accurate reporting

1637. Subsection 122.5(6) will provide a defence to a prosecution 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 and in the person's capacity as a journalist engaged in fair and accurate reporting.

1638. The extension of the defence to a person who deals with or holds information is intended to allow journalists to undertake a range of activities that are necessary in the course of fair and accurate public interest journalism. For example, journalists must obtain or collect information from a source, hold and deal with that information the course of researching and preparing a story, and deal with that information in course of consulting with editors, experts and relevant Australian Government officials to satisfy the journalist as to the appropriate

balance between competing public interests. Additionally, the extension for the defence to a person who holds information is intended to enable journalists to perform the important function of 'filtering' stories that are contrary to the public interest. From time-to-time, journalists may obtain or collect information from sources, and determine that it would be contrary to the public interest to publish some or all of that information. For example, in some cases, the public interest may be fully served by publishing a certain amount of information, whereas the publication of further information or particular details may, on balance, be contrary to the public interest. It is intended that journalists should be permitted to deal with information, and then determine to either publish the information, or to hold the information rather than to publish the information.

1639. The term 'journalist' should take its ordinary and natural meaning. For example, the Macquarie Dictionary defines 'journalist' as being a person engaged in 'journalism', being 'the business or occupation of writing, editing, and producing photographic images for print media and the production or news and news analysis for broadcast media'. Similarly, the Oxford Dictionary defines 'journalist' as 'a person who writes for newspapers, magazines, or news websites or prepares news to be broadcast'. A journalist need not be regularly employed in a professional capacity, and may include a person who self-publishes news or news analysis.

1640. 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.

1641. 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.

1642. The Note under the defence at subsection 122.5(6) clarifies that the defendant will bear an evidential burden in relation to this defence. Section 13.3 of the Criminal Code provides that in the case of a standard 'evidential burden' defence, the defendant bears the burden of pointing to evidence that suggests a reasonable possibility that the defence is made out. If this is done, the prosecution must refute the defence beyond reasonable doubt (section 13.1). The imposition of the evidential burden on the defendant is appropriate because the defendant should be readily able to point to evidence founding a suggestion that there is a reasonable possibility that their conduct was done in the public interest and in their capacity as a journalist engaged in fair and accurate reporting. Additionally, requiring the prosecution to prove beyond reasonable doubt that a person's conduct was not for such a purpose would often prove an insurmountable barrier to a successful prosecution, undermining the deterrent effect of the new general secrecy offences.

Information that has been previously communicated

1643. Subsection 122.5(8) will provide a defence to a prosecution for an offence relating to the communication of information, if there has been a prior publication of that information in certain circumstances. A person will not be criminally liable if:

- the person did not make or obtain the information by reason of any of the following:
    - his or her being, or having been, a Commonwealth officer
    - his or her being otherwise engaged to perform work for a Commonwealth entity
    - an arrangement or agreement to which the Commonwealth or a Commonwealth entity is party and which allows for the exchange of information
- the information has already been communicated, or made available, to the public (the prior publication)
- the person was not involved in the prior publication (whether directly or indirectly)
- at the time of the communication, the person believes that the communication will not cause harm to Australia's interests or the security or defence of Australia, and
- having regard to the nature, extent and place of the prior publication, the person has reasonable grounds for that belief.

1644. The defence is drafted in similar terms to the prior publication defence contained in subsection 35P(3A) of the ASIO Act. Subsection 35P(3A) was inserted following the recommendation of the then- Independent National Security Legislation Monitor, the Hon Roger Gyles AO QC, in his *Report on the impact on journalists of the operation of section 35P of the ASIO Act*, which was tabled in the Parliament on 2 February 2016.

1645. It is intended that paragraph 122.5(8)(a) will limit the availability of the defence to individuals who did not receive the relevant information in an official capacity. Persons who have received information in their official capacity will not be criminally liable for communicating or dealing with the information in their official capacity, by reason of the defence in subsection 122.5(1). The limitation of the prior publication defence in subsection 122.5(8) to persons who did not receive the relevant information in an official capacity is consistent with the Monitor's recommendation, and the drafting of subsection 35P(3A).

1646. The defence under subsection 122.5(8) 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. For example, this would be the case where information is brought into the public domain inadvertently, such as where a security classified document or information provided to the Australian Government in accordance with a legal obligation is revealed as a result of a technical or administrative error. Where steps are quickly taken to reverse the disclosure, subsequent publication of that information is likely to bring that information to the attention of a much greater number of people and could result in considerable new or additional harm.

1647. The Note under the defence at subsection 122.5(8) clarifies that the defendant will bear an evidential burden in relation to this defence. Section 13.3 of the Criminal Code provides that in the case of a standard 'evidential burden' defence, the defendant bears the burden of pointing to evidence that suggests a reasonable possibility that the defence is made out. If this is done, the prosecution must refute the defence beyond reasonable doubt (section 13.1). The imposition of the evidential burden on the defendant is appropriate because the defendant should be readily able to point to evidence founding a suggestion that there is a reasonable possibility that they did not receive the information in an official capacity, the information has already been communicated, or made available, to the public, that the person was not involved in the prior publication, and that they believed on reasonable grounds that their communication would not cause harm to Australia's interests or the security or defence of Australia.

Information relating to a person etc.

1648. Subsection 122.5(9) will provide a defence to a prosecution for an offence relating to dealing with information if:

- the person did not make or obtain the information by reason of any of the following:
    - his or her being, or having been, a Commonwealth officer

    - his or her being otherwise engaged to perform work for a Commonwealth entity

    - an arrangement or agreement to which the Commonwealth or a Commonwealth entity is party and which allows for the exchange of information, and

- at the time of the dealing, the person believes that the making or obtaining of the information by the person was required or authorised by law

- having regard to the circumstances of the making or obtaining of the information, the person has reasonable grounds for that belief, and

- any of the following apply:

    - the person communicates the information to the person to whom the information relates

    - the person is the person to whom the information relates

    - the dealing is in accordance with the express or implied consent of the person to whom the information relates.

1649. The offences in Division 122 are not intended to prevent a person from dealing in information that relates to them, or to limit the ability of a person to consent to another person dealing information that relates to them. The following are examples of situations in which it is intended that the defence in subsection 122.5(9) would ensure that a person is not criminally liable for dealing in information:

- Example 1: Person A give taxation information to the Australian Taxation Office as part of their income tax return, as required by section 161 of the *Income Tax Assessment Act 1936*. Person A then communicates the same information to their bank, as part of an application for a mortgage.

- Example 2: Person B is the accountant for Person C. Person B has lodged Person C's income tax return on Person C's behalf. Person B gives Person C a copy of the tax return as lodged.

- Example 3: Person D has received a notice issued under an Act requiring them to provide a Commonwealth agency with information that relates to Person D. Person D gives the agency the information specified in the notice. The Act does not contain a specific secrecy provision limiting the disclosure of information about the notice. Person D subsequently shows Person E the notice and the information that Person D gave to the agency in accordance with the notice.

1650. Paragraph 122.5(9)(a) limits the application of the defence in relation to persons who have made or obtained the relevant information in an official capacity, or under an agreement or arrangement allowing for the exchange of information. Persons who have made or obtained information in such circumstances are under a higher duty to protect that information. It is intended that such persons should deal with information under other

defences contained in section 122.5 and Part 2.3 of the Criminal Code. In particular, persons who have made or obtained information in an official capacity or under an agreement or arrangement should deal with that information pursuant to subsection 122.5(1), in the course of performing their functions or duties in their official capacity, or in accordance with the agreement or arrangement.

- Example: Person A is an employee of the Australian Federal Police. Person A is investigating Person B, who is reasonably suspected of being involved in various organised criminal activities. Person A communicates information about the status of that investigation to Person B (being the person to whom the information relates). Person A would not be able to rely on the defence at subsection 122.5(9) because the information was obtained due to Person A's role as a Commonwealth official.

1651. Paragraphs 122.5(9)(b) and (c) provide that the defence will only be available where:

- at the time of the dealing, the person believes that the making or obtaining of the information by the person was required or authorised by law, and

- having regard to the circumstances of the making or obtaining of the information, the person has reasonable grounds for that belief.

1652. Paragraphs (b) and (c) are intended to ensure that persons who act as intermediaries for the unlawful disclosure of information to persons to whom the information relates (such as information about an investigation into a person) do not benefit from the defence.

- Example: Person C is an employee of the Australian Federal Police. Person C is investigating Person D, who is reasonably suspected of being involved in various organised criminal activities. Person C meets Person E in a bar, gives Person E a file containing information about the status of the investigation, requests that Person E pass the information to Person D, and warns Person E to take precautions to not be detected or they could both be arrested. Person E communicates the information to Person D (being the person to whom the information relates). Person E would not be able to rely on the defence at subsection 122.5(9) because, in all of the circumstances, Person E could not reasonably believe that the person's obtaining of the information was required or authorised by law.

Division 123—Miscellaneous

Section 123.1—Injunctions

1653. Subsection 123.1(1) provides that the provisions of Division 122 are enforceable under Part 7 of the *Regulatory Powers (Standard Provisions) Act 2014*. Part 7 of the Act creates a standard framework for the use of injunctions in the enforcement of provisions.

1654. Injunctions may be used to restrain a person from contravening a provision of Division 122.

1655. Paragraph 123.1(2)(a) provides that the Minister is an authorised person for the purposes of Part 7 of the *Regulatory Powers (Standard Provisions) Act 2014*, as that part

applies to the provisions of Division 122. The effect of paragraph (2)(a) is that the Minister may apply to a relevant court for an injunction to restrain a person from committing an offence against section 122.1, 122.2, 122.3 or 122.4.

1656. Paragraph 123.1(2)(b) provides that the Federal Court of Australia, the Federal Circuit Court of Australia, and a court of a State or Territory that has jurisdiction in relation to matters arising under the *Criminal Code Act 1995*.

1657. Subsection 123.1(3) provides that Part 7 of the Regulatory Powers Act, as that Part applies to the provisions of Division 122, extends to every external Territory. The offences in Division 122 have Category D extended geographic application and therefore extend *inter alia* to every external Territory; accordingly, it is appropriate that injunctions under Part 7 also be available in the external Territories to restrain contraventions of Division 122.

Section 123.2—Forfeiture of articles

1658. Section 123.2 provides that a sketch, article, record or document which is made, obtained, recorded, retained, possessed or otherwise dealt with in contravention of Part 5.6 is forfeited to the Commonwealth. ***Sketch***, ***article*** and ***record*** have the same respective meanings as in Part 5.2.

1659. Section 123.2 substantially replicates section 85D of the Crimes Act and is intended to prevent or minimise the harm to essential public interests arising from the unlawful communication, dealing with, removal or holding of inherently harmful information or information, the communication of which would cause harm to Australia's interests. The forfeiture of a sketch, article, record or document which is made, obtained, recorded, retained, possessed or otherwise dealt with in contravention of Part 5.6 is intended to prevent or minimise the further communication or dealing with information contained in such sketches, articles, records or documents.

1660. It is appropriate that a sketch, article, record or document which is made, obtained, recorded, retained, possessed or otherwise dealt with in contravention of Part 5.6 is automatically forfeited to the Commonwealth by operation of law. The offences in Part 5.6 are intended to protect essential public interests, by criminalising the unlawful communication and dealing with inherently harmful information, or information the communication of which would cause harm to Australia's interests. Any delay in the recovery of such information would produce an unacceptable risk of harm to essential public interests.

1661. The intended operation of section 123.2 can be contrasted to the intended operation of the forfeiture framework in the *Proceeds of Crime Act 2002*. This section is intended to prevent or minimise harm to essential public interests, whereas the proceeds of crime framework is intended to ensure that criminals are deprived of the benefits of their crime.

Section 123.3—Extended geographical jurisdiction—category D

1662. Section 123.3 applies Section 15.4 (extended geographical jurisdiction—Category D) to each offence against Part 5.6 (Secrecy). Under section 15.4, the effect of Category D geographical jurisdiction is that the offence applies:

- whether or not the conduct constituting the alleged offence occurs in Australia, and

- whether or not a result of the conduct constituting the alleged offence occurs in Australia.

1663. Category D jurisdiction is appropriate because:

- inherently harmful information, and information the communication of which would cause harm to Australia's interests, may be communicated or dealt with outside of Australia—for example, where an employee of a Commonwealth department removes information from Australia before communicating it;

- inherently harmful information, and information the communication of which would cause harm to Australia's interests, may itself be held outside Australia—for example, where the Australian Defence Force is deployed overseas;

- the harms that may result from the disclosure of inherently harmful information, or information the communication of which may cause harm to Australia's interests, may occur outside Australia—for example, where the information relates to the security of Australian Defence Force or diplomatic personnel overseas, or to Australian companies or citizens operating or travelling in foreign countries.

Item 7 - Application

1664. This item provides that the amendments made by Part 1 of Schedule 2 of the Bill apply to conduct that occurs on or after the commencement of this item.

PART 2 – CONSEQUENTIAL AMENDMENTS

Agricultural and Veterinary Chemicals (Administration) Act 1992

Item 8

1665. Section 69F of the *Agricultural and Veterinary Chemicals (Administration) Act 1992* deals with the appointment of inspectors, and persons authorised to exercise the powers and perform the functions of inspectors, for purposes of a relevant law under the Act. Subsection 69F(3) provides that an inspector is a Commonwealth officer for the purposes of section 70 of the Crimes Act. Section 70 is being repealed by Item 5 of Schedule 2 and replaced by new secrecy provisions to be included in Part 5.6 of the Criminal Code.

1666. Item 8 repeals the reference to section 70 from section 69F and replaces it with a reference to new Part 5.6 of the Criminal Code (to be inserted by Item 6 of Schedule 2). This ensures that inspectors under the *Agricultural and Veterinary Chemicals (Administration) Act 1992* are considered to be Commonwealth officers for the purposes of the new secrecy offences.

Archives Act 1989

Item 9

1667. Section 30A(1) of the *Archives Act 1989* imposes a duty on Archives officers not to divulge or communicate any Census information to another person, except to another Archives officer for the purposes of, or in connection with, the performance of that other officer's duties arising under the Act. The note to subsection 30A(1) refers to section 70 of the Crimes Act, which is being repealed by Item 5 of Schedule 2.

1668. The new section 122.4 (to be inserted by Item 6 of Schedule 2) creates an offence, based on the existing section 70, that applies where a person communicates information that is made or obtained by reason of him or her being, or having been, a commonwealth officer or otherwise engaged in work for the Commonwealth, and where the person is under a duty, arising under a law of the Commonwealth, not to disclose the information.

1669. Item 9 amends the Note to section 30A(1) to remove the reference to section 70 of the Crimes Act and substitute it with a reference to the new section 122.4 of the Criminal Code.

Australian Citizenship Act 2007

Items 10 and 11

1670. Paragraph (a) of the definition of 'national security offence' in section 3 of the *Australian Citizenship Act 2007* refers to offences against Part VII of the Crimes Act. Part VII of the Crimes Act will be repealed by Item 5 of Schedule 2 and replaced with new secrecy provisions to be included in Part 5.6 of the Criminal Code.

1671. Items 10 and 11 amend the definition of national security offence in section 3 to repeal the existing reference to Part VII and insert a reference to Part 5.6 of the Criminal Code.

Australian Crime Commission Act 2002

Item 12

1672. Schedule 1 (entry relating to the *Australian Intelligence Organisation Act 1979*) of the *Australian Crime Commission Act 2002* refers to '*Crimes Act 1914*, section 85B'. Section 85B, which relates to hearings in camera, is being repealed by Item 5 of Schedule 2.

1673. Item 12 repeals the words '*Crimes Act 1914*, section 85B' from Schedule 1.

Australian Federal Police Act 1979

Items 13 and 14

1674. Subparagraph (a)(i) of the definition of 'protective service offence' in subsection 4(1) of the *Australian Federal Police Act 1979* refers to an offence under section 79 of the Crimes Act. Section 79 of the Crimes Act is being repealed by Item 5 of Schedule 2 and will be replaced by new secrecy provisions to be included in Part 5.6 of the Criminal Code.

1675. Items 13 and 14 amend the definition of protective service offence in subsection 4(1) to repeal the existing reference to section 79 and insert a reference to Part 5.6 of the Criminal Code.

Chemical Weapons (Prohibition) Act 1994

Item 15

1676. Section 102 of the *Chemical Weapons (Prohibition) Act 1994* creates a number of non-disclosure duties that apply to an 'eligible person', which is defined in subsection 102(1) to include a person who is or has been a Commonwealth officer. Subsection 102(5) provides that a 'Commonwealth officer has the same meaning as in section 70 of the *Crimes Act 1914*'.

1677. Section 70 of the Crimes Act is being repealed by Item 5 of Schedule 2 and will be replaced by new secrecy provisions to be included in Part 5.6 of the Criminal Code. A new definition of 'Commonwealth officer' will be created in section 121.1, to be inserted by Item 6 of Schedule 2.

1678. Item 15 will amend subsection 102(5) to repeal the reference to section 70 of the Crimes Act and substitute the new definition of 'Commonwealth officer' in section 121.1 of the Criminal Code.

Comprehensive Nuclear-Test-Ban Treaty Act 1998

Item 16

1679. Section 74 of the *Comprehensive Nuclear-Test-Ban Treaty Act 1998* creates a number of non-disclosure duties that apply to persons specified in subsection 74(1), which includes a person who is or has been a Commonwealth officer (within the meaning of section 70 of the Crimes Act) (see paragraph 71(4)(e)).

1680. Section 70 of the Crimes Act will be repealed by Item 5 of Schedule 2 and will be replaced by new secrecy provisions to be included in Part 5.6 of the Criminal Code.

1681. Item 16 will amend paragraph 71(4)(e) to repeal the reference to section 70 and substitute the new definition of 'Commonwealth officer' that will be created by section 121.1 of the Bill.

Defence Home Ownership Assistance Scheme Act 2008

Item 17

1682. Subsection 81(5) of the *Defence Home Ownership Assistance Scheme Act 2008* provides that employees of the authorised Commonwealth contractor exercising functions and powers delegated under the Act are to be prohibited from unauthorised disclosure of information in the same way as Commonwealth officers are prohibited from the unauthorised disclosure of official information under section 70 of the Crimes Act. Section 70 of the Crimes Act will be repealed by Schedule 2 of the Bill and replaced by new secrecy provisions to be included in Part 5.6 of the Criminal Code.

1683. Item 17 repeals subsection 81(5). The new definition of 'Commonwealth officer' in section 121.1 (to be inserted by Item 6 of Schedule 2) will apply to persons acting under the *Defence Home Ownership Assistance Scheme Act 2008*.

Freedom of Information Act 1982

Item 18

1684. Subsection 78(2) of the *Freedom of Information Act 1982* requires approval to be sought before an authorised person can enter or carry on an investigation at a place referred to in paragraph 80(c) of the Crimes Act (see paragraph 78(1)(a)).

1685. Declarations were made by the Governor-General under section 80(c) between 1959 and 1986. The declarations, which mainly relate to Defence premises, are archaic and have not been updated or used for many years. Section 80 of the Crimes Act is being repealed by Schedule 2 of the Bill.

1686. Item 18 will repeal paragraph 78(1)(a) to remove the reference to paragraph 80(c) of the Crimes Act.

Law Enforcement Integrity Commissioner Act 2006

Item 19

1687. Subsection 105(3) of the *Law Enforcement Integrity Commissioner Act 2006* requires approval to be sought before the Law Enforcement Integrity Commissioner can enter or carry on an investigation at a place referred to in paragraph 80(c) of the Crimes Act. Section 80 of the Crimes Act is being repealed by Schedule 2 of the Bill.

1688. Declarations were made by the Governor-General under section 80(c) between 1959 and 1986. The declarations, which mainly relate to Defence premises, are archaic and have not been updated or used for many years. Section 80 of the Crimes Act is being repealed by Schedule 2 of the Bill.

1689. Item 19 will repeal subsection 105(3) to remove the reference to paragraph 80(c) of the Crimes Act.

Liquid Fuel Emergency Act 1984

Item 20

1690. Section 29 of the *Liquid Fuel Emergency Act 1984* provides for the appointment of authorised persons for the purposes of the Act. Subsection 29(3) provides that authorised persons are taken to be Commonwealth officers within the meaning of Part VI of the Crimes Act.

1691. Part VI of the Crimes Act is being repealed by Item 5 of Schedule 2.

1692. Item 20 repeals subsection 29(3). The new definition of 'Commonwealth officer' in section 121.1 (to be inserted by Item 6 of Schedule 2) will apply to persons appointed under the *Liquid Fuel Emergency Act 1984*.

Migration Act 1958

Item 21

1693. Subsection 503(9) of the Migration Act protects information supplied by law enforcement agencies or intelligence agencies. Section 503 refers to the definition of 'Commonwealth officer' in section 70 of the Crimes Act, which will be repealed by Item 5 of Schedule 2 of the Bill.

1694. Item 21 amends subsection 503(9) to repeal the reference to section70 and substitute the new definition of 'Commonwealth officer' in section 121.1 of the Criminal Code.

National Greenhouse and Energy Reporting Act 2007

Item 22

1695. Under subsection 23(1) of the *National Greenhouse and Energy Reporting Act 2007* it is an offence for a person to disclose information in contravention of section 23(1). The Note to subsection 23(1) clarifies that the same conduct may be an offence against both subsection 23(1) and section 70 of the *Crimes Act 1914*.

1696. Section 70 of the Crimes Act is being repealed by Item 5 of Schedule 2 and will be replaced by new secrecy provisions to be included in Part 5.6 of the Criminal Code.

1697. New section 122.4 (to be inserted by Item 6 of Schedule 2) creates an offence, based on the existing section 70, that applies where a person communicates information that is made or obtained by reason of him or her being, or having been, a commonwealth officer or otherwise engaged in work for the Commonwealth, and where the person is under a duty, arising under a law of the Commonwealth, not to disclose the information.

1698. Item 22 amends the Note to section 23(1) to remove the reference to section 70 of the Crimes Act and substitute it with a reference to the new section 122.4 of the Criminal Code.

Item 23

1699. Section 57 of the *National Greenhouse and Energy Reporting Act 2007* deals with the appointment of an authorised officer under the Act. Section 57(2) provides that in exercising powers or performing functions as an authorised officer, an authorised officer must comply with any directions of the Regulator. The Note to subsection 57(2) refers to section 70 of the *Crimes Act 1914*.

1700. Section 70 of the Crimes Act is being repealed by Item 5 of Schedule 2 and will be replaced by new secrecy provisions to be included in Part 5.6 of the Criminal Code.

1701. New section 122.4 (to be inserted by item 8 of Schedule 2) creates an offence, based on the existing section 70, that applies where a person communicates information that is made or obtained by reason of him or her being, or having been, a commonwealth officer or otherwise engaged in work for the Commonwealth, and where the person is under a duty, arising under a law of the Commonwealth, not to disclose the information.

1702. Item 23 amends the Note to section 57(2) to remove the reference to section 70 of the Crimes Act and substitute it with a reference to the new section 122.4 of the Criminal Code.

Native Title Act 1993

Item 24

1703. Section 203DF of the *Native Title Act 1993* provides for the appointment of a person to perform inspections and audits or undertake investigations under the Act, as specified in subsection 203DF(1). Subsection 203DF(8) clarifies that, to avoid doubt, a person appointed under subsection 203DF(1) is taken to be a 'Commonwealth officer', for the purposes of section 70 of the Crimes Act.

1704. Section 70 of the Crimes Act is being repealed by Item 5 of Schedule 2 and will be replaced by new secrecy provisions to be included in Part 5.6 of the Criminal Code.

1705. The new section 122.4 (to be inserted by Item 6 of Schedule 2) creates an offence, based on the existing section 70, that applies where a person communicates information that is made or obtained by reason of him or her being, or having been, a commonwealth officer or otherwise engaged in work for the Commonwealth, and where the person is under a duty, arising under a law of the Commonwealth, not to disclose the information.

1706. Item 24 repeals subsection 2203DF(8). The new definition of 'Commonwealth officer' in section 121.1 (to be inserted by Item 6 of Schedule 2) will apply to persons appointed under the *Native Title Act 1993*.

Offshore Minerals Act 1994

Item 25

1707. Subsection 405 of the *Offshore Minerals Act 1994* sets out the general regime for criminal offences under the Act. Subsection 405(2) specifies that Crimes Act and the Criminal Code contain provisions that are relevant to the operation of the Act and Note 3 to subsection 405(2) contains a reference to the general offence of unauthorised disclosure under section 70 of the Crimes Act.

1708. Section 70 of the Crimes Act will be repealed by Item 5 of Schedule 2 and replaced by new secrecy provisions to be included in Part 5.6 of the Criminal Code.

1709. Item 25 amends the note to subsection 405(2) to remove the existing reference to section 70 of the Crimes Act and substitute it with a reference to the new secrecy offences in Part 5.6 of the Criminal Code.

Ombudsman Act 1976

Item 26

1710. Paragraph 14(2)(a) of the *Ombudsman Act 1976* deals with powers under the Act to enter premises in order to undertake investigations. Subparagraph 14(2)(a)(i) requires the Ombudsman to seek approval before entering or carrying on an investigation at a 'prohibited place' referred to under paragraph 80(c) of the Crimes Act. Section 80 of the Crimes Act is being repealed by Schedule 2 of the Bill.

1711. Declarations were made by the Governor-General under section 80(c) between 1959 and 1986. The declarations, which mainly relate to Defence premises, are archaic and have

not been updated or used for many years. Section 80 of the Crimes Act is being repealed by Schedule 2 of the Bill.

1712. Item 26 repeals subparagraph 14(2)(a)(i) to remove the reference to paragraph 80(c) of the Crimes Act.

Parliamentary Service Act 1999

Items 27 and 28

1713. Subsections 65AA(2) and 65AB(2) of the *Parliamentary Service Act 1999* prohibits the unauthorised disclosure or other use of protected information by a person who is an entrusted person under the Act. Protected information and entrusted person are defined in subsections 65AA(1) and 65AB(1). Both subsections 65AA(2) and 65AB(2) contain Notes referring to the secrecy offence at section 70 of the Crimes Act.

1714. Section 70 of the Crimes Act is being repealed by Item 5 of Schedule 2 and will be replaced by new secrecy provisions to be included in Part 5.6 of the Criminal Code.

1715. New section 122.4 (to be inserted by Item 6 of Schedule 2) creates an offence, based on the existing section 70, that applies where a person communicates information that is made or obtained by reason of him or her being, or having been, a commonwealth officer or otherwise engaged in work for the Commonwealth, and where the person is under a duty, arising under a law of the Commonwealth, not to disclose the information.

1716. Items 27 and 28 will amend the Notes to subsections 64AA(2) and 65AB(2) to remove the existing references to section 70 of the Crimes Act and substitute references to new section 122.4 of the Criminal Code.

Public Service Act 1999

Items 29 and 30

1717. Subsections 72A(2) and 72B(2) of the *Public Service Act 1999* prohibit the unauthorised disclosure or other use of protected information by a person who is an entrusted person under the Act. 'Protected information' and 'entrusted person' are defined in subsections 72A(1) and 72B(1). Both subsections 72A(2) and 72B(2) contain Notes referring to the secrecy offence at section 70 of the Crimes Act.

1718. Section 70 of the Crimes Act is being repealed by Item 5 of Schedule 2 and will be replaced by new secrecy provisions to be included in Part 5.6 of the Criminal Code.

1719. The new section 122.4 (to be inserted by item 8 of Schedule 2) creates an offence, based on the existing section 70, that applies where a person communicates information that is made or obtained by reason of him or her being, or having been, a commonwealth officer or otherwise engaged in work for the Commonwealth, and where the person is under a duty, arising under a law of the Commonwealth, not to disclose the information.

1720. Item 29 and 30 will amend subsections 72A(2) and 72B(2) to remove references to section 70 of the Crimes Act and replace them with a references to the new section 122.4 of the Criminal Code.

Renewable Energy (Electricity) Act 2000

Item 31

1721. Section 156 of the *Renewable Energy (Electricity) Act 2000* provides the Clean Energy Regulator with the power to delegate functions and powers under the Act. Subsection 156(4) provides that for the purposes of the definition of Commonwealth officer in section 70 of the Crimes Act, a person who performs functions, or exercises powers, under a delegation under section 154 is taken to be a person who performs services for the Commonwealth.

1722. Section 70 of the Crimes Act will be repealed by Item 5 of Schedule 2 of the Bill and replaced by new secrecy provisions to be included in Part 5.6 of the Criminal Code.

1723. Item 31 will amend subsection 156(4) to repeal the reference to section 70 and substitute the new definition of 'Commonwealth officer' that will be created by section 121.1 of the Bill.

Textile, Clothing and Footwear Investment and Innovation Programs Act 1999

Items 32, 33 and 34

1724. Subsections 37R(6), 37ZZA(6) and 52(5) of the *Textile, Clothing and Footwear Investment and Innovation Programs Act 1999* all refer to the definition of 'Commonwealth officer' in section 70 of the Crimes Act in relation to persons authorised to perform functions, or exercise powers under each of the respective subsections of the Act.

1725. Section 70 of the Crimes Act will be repealed by Item 5 of Schedule 2 of the Bill and replaced by new secrecy provisions to be included in Part 5.6 of the Criminal Code.

1726. Items 32, 33 and 34 will amend subsections 37R(6), 37ZZA(6) and 52(5) of the Textile, Clothing and Footwear Investment and Innovation Programs Act repeal the reference to section 70 and substitute the new definition of 'Commonwealth officer' that will be created by section 121.1 of the Bill.

SCHEDULE 3 – AGGRAVATED OFFENCE FOR GIVING FALSE OR MISLEADING INFORMATION

General Outline

1727. Schedule 3 amends Division 137 of Part 7.4 of the Criminal Code to introduce a new aggravated offence that applies where a person provides false or misleading information in relation to an application for, or maintenance of, an Australian Government security clearance. The introduction of the aggravated offence reflects the serious consequences that can flow from the provision of false or misleading information, or the omission of relevant information, during a security clearance process that could lead to a person gaining access to highly classified information.

Criminal Code Act 1995

Item 1

1728. Item 1 inserts a new aggravated offence for giving false or misleading information after section 137.1 of the Criminal Code.

Section 137.1A – Aggravated offence for giving false or misleading information

1729. Subsection 137.1A(1) creates an aggravated offence for giving false or misleading information. The aggravated offence will apply where a person commits an underlying offence against subsection 137.1(1) (false or misleading information), and the information given in committing the underlying offence was given in relation to an application for, or the maintenance of, an Australian Government security clearance.

1730. The aggravated offence will be punishable by a maximum penalty of five years imprisonment.

1731. Examples of this offence are as follows.

- Person A is seeking employment in a Commonwealth government department and has applied for an Australian Government clearance. On the application form, Person A did not disclose that he had previously participated in military service for a foreign country. As a result of this omission, the Commonwealth agency responsible for security clearances is not aware of Person A's connection with, and possible allegiance to, the armed forces of a foreign country.

- Person A is employed in a Commonwealth government department and holds an Australian government security clearance. The security clearance allows Person A to access highly sensitive, classified information. During an overseas trip to Country X, Person A forms an ongoing association with Person B, who is a citizen of Country X and an employee of the government of Country X. In the maintenance of Person A's security clearance, Person A does not disclose the association with Person B. As a result of Person A's omission, the Commonwealth agency responsible for security clearances is unaware of Person A's association with Person B and Country X.

1732. To establish the aggravated offence, the prosecution will first need to prove, beyond a reasonable doubt, that a person commits the underlying offence. To establish the underlying offence, the prosecution will need to prove, beyond a reasonable doubt, that:

- a person intentionally gives information to another person
- the person knows that the information:
    - is false or misleading; or
    - omits any matter or article without which the information is misleading
- the information is given:
    - to a Commonwealth entity;
    - to a person who is exercising powers or performing functions under, or in connection with, a law of the Commonwealth; or
    - in compliance or purported compliance with a law of the Commonwealth.

1733. In addition to establishing the underlying offence, the prosecution will also need to prove beyond a reasonable doubt that the information given in committing the underlying offence was given in relation to an application for, or the maintenance of, an Australian Government security clearance. Section 5.6 of the Criminal Code will apply the automatic fault element of recklessness to the circumstance in paragraph 137.1A(1)(b). Section 5.4 of the Criminal Code provides that a person is reckless with respect to a circumstance if he or she is aware that the circumstance exists or will exist and, having regard to the circumstances known to him or her, it is unjustifiable to take that risk.

1734. Subsection 137.1A(2) provides that there is no fault element for the physical element in paragraph 137.1A(1)(a) other than the fault elements (however described) for the underlying offence. The underlying offence has specific physical and fault elements that must be proved by the prosecution (as outlined above). The prosecution will be required to establish beyond reasonable doubt all of the elements constituting the relevant underlying offence, including any fault elements applicable to that offence. Subsection 137.1(2) has been included to make clear that for the purposes of the offence in section 137.1A(1), the prosecution does not need to prove any fault elements in addition to those fault elements already applying to the underlying offences.

1735. Paragraph 137.1A(3)(a) provides that, to avoid doubt, a person does not commit the underlying offence for the purposes of paragraph 137.1A(1)(a) if the person has a defence to the underlying offence. This has been included to make clear that a person does not commit the underlying offence, and cannot therefore be found liable under the new aggravated offence at section 137.1A, if a defence applies to the underlying offence.

1736. Section 137.1 includes defences that provide that a person does not commit the offence if:

- the information is not false or misleading in a material particular (subsection 137.1(2))

- 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 at section 137.1, for example by using the words 'giving false or misleading information is a serious offence' (subsections 137.1(4)-(6))

1737. Paragraph 137.1A(3)(b) clarifies that a person may be convicted of the new aggravated offence against subsection 137.1A(1) even if the person has not been convicted of the underlying offence at section 137.1. This subsection makes it clear that to be convicted of the aggravated offence a person does not have to be convicted of the underlying offence; rather a person only needs to have committed the underlying offence. In this respect, paragraph 137.1A(1)(a) still requires the prosecution to prove, beyond a reasonable doubt, all elements constituting the underlying offence in order to establish that the aggravated offence has been committed.

1738. Subsection 137.1A(4) provides that if the trier of fact is not satisfied that a person is guilty of the aggravated offence but is satisfied, beyond a reasonable doubt, that the person is guilty of the underlying offence; it may find the person not guilty of the aggravated offence but guilty of the underlying offence. Subsection 137.1A(5) provides that subsection 137.1A(4) only applies if the person has been accorded procedural fairness in relation to the finding of guilt for the underlying offence.

1739. Subsection 137.1A(6) ensures that a reference in any law to section 137.1 (the underlying offence) is taken to include a reference to section 137.1A (the aggravated offence).

1740. The aggravated offence will be punishable by a maximum penalty of five years imprisonment. This penalty reflects the higher level of culpability associated with the provision of false or misleading information in security clearance processes. In such cases, providing false or misleading information concerning links to foreign individuals, entities and governments may be particularly harmful as vetting and security agencies are unable to adequately assess the risks posed by the person seeking an Australian Government security clearance. The penalty for the aggravated offence is consistent with the established principle of Commonwealth criminal law policy as set out in the Guide to Framing Commonwealth Offences to impose a heavier penalty where the consequences of the offence are particularly dangerous or damaging.

SCHEDULE 4 – TELECOMMUNICATIONS SERIOUS OFFENCES

General outline

1741. Schedule 4 amends the definition of a 'serious offence' in subsection 5D(1)(e) of Part 1.2 of the *Telecommunications (Interception and Access) Act 1979* (TIA Act) to include the offences provided for in the Bill. A 'serious offence' for the purpose of the TIA Act is one for which declared agencies can seek interception warrants.

1742. The gravity of the threat posed to Australia's national security by espionage, foreign interference and related activities demonstrates the need to take reasonable steps to detect, investigate and prosecute those suspected of engaging in such conduct. The current lack of law enforcement and intelligence powers with respect to these activities has resulted in a permissive operating environment for malicious foreign actors, which Australian agencies are unable to effectively disrupt and mitigate. Amendments to the TIA Act will ensure declared agencies have access to telecommunications interception powers to investigate the offences provided for in the Bill.

PART 1 – AMENDMENTS COMMENCING AT THE SAME TIME AS SCHEDULES 1 AND 3 TO THIS ACT

Item 1

1743. This item inserts new subparagraphs into the definition of 'serious offence' in paragraph 5D(1)(e) of the TIA Act to cover:

- Division 82 of the Criminal Code (sabotage)
- Division 83 of the Criminal Code (other threats to security)
- Division 91 of the Criminal Code (espionage)
- Division 92 of the Criminal Code (foreign interference), and
- Division 92A of the Criminal Code (theft of trade secrets involving foreign government principal).

1744. The new subparagraphs will be added after subparagraph 5D(1)(e)(ib).

1745. The new subparagraphs extend the meaning of 'serious offence' for the purposes of the TIA Act to include the offences of sabotage, other threats to security, espionage, foreign inference and theft of trade secrets involving foreign government principal.

1746. Telecommunications interception is an essential tool for investigating offences involving foreign principals or communication of sensitive information.

1747. Under subparagraph 5D(1)(e)(ia) of the TIA Act, treason offences are already listed as serious offences.

1748. Subparagraph 5D(1)(e)(ic) will include Division 82 of the Criminal Code (sabotage) in the definition of 'serious offence' for the purposes of the TIA Act. The sabotage offences in Division 80, like the other offences listed in paragraph (e) of the TIA Act, are offences that

jeopardise Australia and its national security interests, and for which prevention and disruption are critical to prevent public harm. The gravity of the threat posed by sabotage is reflected in the serious penalties for the offences, which range from 25 years imprisonment to seven years imprisonment.

1749. Further, some sabotage offences, such as those against section 82.7 (offence of introducing vulnerability with intention as to national security) and 82.8 (offence of introducing vulnerability reckless as to national security) of the Criminal Code, involve criminalised activities that could be conducted exclusively online (for example using the internet to render software vulnerable to exploitation). In these cases, it is necessary for law enforcement to be able to intercept the offending service or telecommunications network to investigate the offence.

1750. Subparagraph 5D(1)(e)(id) will include Division 83 of the Criminal Code (other threats to security) in the definition of 'serious offence' for the purposes of the TIA Act. The offences included in Division 83 of the Criminal Code carry significant penalties of between seven and 20 years imprisonment, recognising the serious harm to Australia's sovereignty, national security and other interests that can result from the conduct constituting the commission of such an offence. The severity of offending conduct is particularly dangerous when it is directed or controlled by, or on behalf of, a foreign principal. In such cases, the offender's communication with a foreign principal may occur exclusively online or through telecommunications technology, making interception powers critical in investigation.

1751. Finally, society's increasing reliance on electronic communication means that an offence under Division 83 can easily be perpetrated using a telecommunications network (for example, interfering with a person's democratic rights by making threats online). In these cases, it is necessary for law enforcement to be able to intercept the offending service to investigate the offence.

1752. Subparagraph 5D(1)(e)(ie) will include Division 91 of the Criminal Code (espionage) in the definition of 'serious offence' for the purposes of the TIA Act. Espionage is one of the most serious offences on the Commonwealth statute book, with commensurately high penalties. Espionage involves serious threats to Australia's defence and security. In some circumstances espionage may only be detected through the use of telecommunications interception powers, such as where a person is dealing with hard copy information. These powers will also be critical in identifying and understanding the link to a foreign principal. In the modern context, electronic means present the most common and convenient method of passing information to a foreign principal, making it necessary for investigators to have the option to intercept such communications to prevent serious harm.

1753. Subparagraph 5D(1)(e)(if) will include Division 92 of the Criminal Code (foreign interference) in the definition of 'serious offence' for the purposes of the TIA Act. Foreign interference is similar in nature to espionage, and the consequences of such behaviour can be equally as harmful. As with espionage, the primary means of communication with the foreign principal that a person is directed or controlled by, or acting on behalf of, may be through electronic means. Therefore, it is necessary that law enforcement have the powers and mechanisms available to properly investigate such criminal activity.

1754. Subparagraph 5D(1)(e)(ig) will include Division 92A of the Criminal Code (theft of trade secrets involving foreign government principals) in the definition of 'serious offence' for the purposes of the TIA Act. Theft of trade secrets amounts to economic espionage and

can severely damage Australia's national security and economic interests, warranting a serious penalty of 15 years imprisonment. In the modern context, trade secrets information may be created and stored wholly, or partially, online. It follows that the stealing of such information can also be conducted or facilitated exclusively through electronic means. In such circumstances, it will be critical for law enforcement to be able to use interception powers to investigate this criminal activity.

Item 2

1755. Item 2 inserts new subparagraph (viii) at the end of the definition of serious offence in paragraph 5D(1)(e) in relation to section 137.1A of the Criminal Code (aggravated offence for giving false or misleading information).

1756. Subparagraph 5D(1)(e)(viii) will include section 137.1A of the Criminal Code (aggravated offence for giving false or misleading information) in the definition of 'serious offence for the purposes of the TIA Act. Interception of telecommunications provides a critical mechanism to determine a person's intention in omitting or lying about certain details in the security clearance process. It may also be central in identifying more serious unlawful conduct for example, a person may be lying on a security clearance to cover up more serious criminal activity such as espionage or foreign interference).

1757. An example of this is as follows. A person who holds an Australian Government security clearance may deliberately omit travel details and contact with foreign nationals from high-threat countries from security clearance processes. These false statements result in continuation of the security clearance, which would not have occurred otherwise, undermining the security of the Australian Government agency for which the person works, and partner agencies confidence in the Australian Government.

1758. Telecommunications interception would be critical in understanding the person's intentions, associations, and any other prejudicial or unlawful activity threatening Australia's national security. This may include an admission where the offender confirms his or her effort to mislead or provide false information, or where the offender seeks direction or guidance from others involved (such as a foreign intelligence service). It may also identify the involvement of others in similar conduct, including other clearance holders, which, if undetected, would pose a severe national security risk.

1759. Telecommunications interception would provide a critical mechanism to determine the applicant's intention in omitting these details and the nature and extent of the training itself. It may be that an offender seeks direction or guidance from another party (e.g. an intermediary or handler) after being asked direct questions by vetting authorities about their links to a foreign principal. It is necessary, where appropriate, that law enforcement have the mechanism available to take reasonable steps to detect, investigate and prosecute those suspected of such conduct.

PART 1 – AMENDMENTS COMMENCING AT THE SAME TIME AS SCHEDULE 2 TO THIS ACT

Item 1

1760. Item 1 inserts new subparagraph (vii) at the end of the definition of serious offence in paragraph 5D(1)(e) in relation to Division 122 of the Criminal Code (secrecy of information).

1761. Subparagraph 5D(1)(e)(vii) will include Division 122 of the Criminal Code (secrecy of information) in the definition of 'serious offence' for the purposes of the TIA Act. Protecting Australia from espionage and foreign interference relies heavily on strong protections for government information. Therefore, it is important to have robust secrecy laws in place to protect against unauthorised disclosure and handling that could cause harm.

1762. In the modern context, espionage may begin with the passage of government information in a way that would constitute a secrecy offence, but which falls short of an espionage offence (for example, because the person passing the information may not yet have formed an intention to prejudice Australia or to give an advantage to a foreign principal). As with espionage, in some circumstances a secrecy offence may only be detected through the use of interception powers, such as where a person is dealing with hard copy information and such powers will be critical in identifying and understanding a person's dealings with that information (for example, a person may have a conversation with a publisher indicating that they hold a hard copy of sensitive information that will inform a book they are writing). Further, electronic means present the most common and convenient method of passing information. Therefore, it is critical that investigators can intercept such communications to prevent serious harm.

SCHEDULE 5 – FOREIGN INFLUENCE TRANSPARENCY SCHEME

General outline

1763. 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.

1764. Clause 2 provides Part 1 of Schedule 5 will commence at the same time as the *Foreign Influence Transparency Scheme Act 2017* commences. If that Act does not commence, then that Part will not commence at all.

1765. Clause 2 also provides that Part 2 of Schedule 5 will commence immediately after the commencement of the *Foreign Influence Transparency Scheme Act 2017*, or immediately after the commencement of Part 1 of Schedule 1 to the *Electoral Legislation Amendment (Electoral Funding and Disclosure Reform) Act 2017*, whichever is the later to occur. If either Act does not commence, then Part 2 of Schedule 5 will not commence.

PART 1 – TRANSITIONAL PROVISIONS

Item 1

1766. This item makes amendments to the requirement to register under section 16 of the Foreign Influence Transparency Scheme Act. Section 16 requires a person to apply to the Secretary for registration under the scheme within 14 days of becoming liable to register.

1767. This item provides that, if a registrable arrangement is in existence between a person and a foreign principal at the time of the commencement of the Foreign Influence Transparency Scheme Act, the person is not required to register under the scheme before six months after the day on which that Act commences. The effect of this item is that the person must apply to the Secretary for registration within 14 days after the end of the six month period.

1768. This item does not prevent a person from applying to the Secretary for registration under the scheme before the six month period has ended. It is intended to allow persons with existing arrangements with foreign principal's time to arrange their affairs and ensure they comply with the scheme.

1769. If a person and a foreign principal establish an arrangement after the commencement of the Foreign Influence Transparency Scheme Act, section 16 will not be affected by this item and the person will be required to register within 14 days of establishing the arrangement.

PART 2 – AMENDMENTS RELATING TO THE ELECTORAL LEGISLATION AMENDMENT (ELECTORAL FUNDING AND DISCLOSURE REFORM) ACT 2017

Foreign Influence Transparency Scheme Act 2017

Item 2

1770. This item amends the definition of 'electoral donations threshold' set out at section 10 of the Foreign Influence Transparency Scheme Act, to omit the reference to "$13,500" and substitute it with "the disclosure threshold within the meaning of Part XX of the *Commonwealth Electoral Act 1918* (electoral funding and financial disclosure)."

1771. This amendment will ensure that thresholds regarding disbursements of money and other things of value regulated by the Foreign Influence Transparency Scheme Act and the Commonwealth Electoral Act are aligned. If the disclosure threshold under the Commonwealth Electoral Act changes, the electoral donations threshold under the Foreign Influence Transparency Scheme Act will change to match that threshold.

Item 3

1772. 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.

1773. 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.

1774. 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:

1775. 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.

1776. 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.

Item 4

1777. This item amends subsection 12(1) of the *Foreign Influence Transparency Scheme Act 2017* to expand the circumstances in which an activity is done for the purpose of 'political or governmental influence.' Whether an activity is done for the purpose of 'political or governmental influence' is relevant to a number of provisions of that Act, including whether a person will be liable to register under the scheme.

1778. The item inserts new paragraph (g) which reads "processes in relation to a person or entity registered under the Commonwealth Electoral Act as a political campaigner." The effect of this insertion is that if a person undertakes an activity for the purpose of influencing a process in relation to a registered political campaigner, that activity will be taken to have been done for a purpose of 'political or governmental influence,' and may attract a requirement to register under the scheme.

1779. This item amends section 12 of the Foreign Influence Transparency Scheme Act to provide a number of examples of processes in relation to a registered political campaigner for the purposes of paragraph 12(1)(g). The examples, to be included in subsection 12(7) are:

- processes in relation to the campaigner's:
    - constitution
    - platform
    - policy on any matter of public concern
    - administrative or financial affairs (in his or her capacity as a campaigner, if the campaigner is an individual)
    - membership, or
    - relationship with foreign principals or with bodies controlled by such foreign principals;
- the conduct of the campaigner's campaign
- the selection (however done) of officers of the campaigner's executive or delegates to its conferences,
- the selection (however done) of the campaigner's leader and any spokespersons for the campaigner.

1780. The above examples are not an exhaustive list of processes in relation to a registered political campaigner. The examples are not intended to limit the scope or application of this section in any way, but have been included to assist readers with the interpretation of the provisions in the Foreign Influence Transparency Scheme Act.

1781. An example of an activity for the purpose of influencing a process of a registered political campaigner is lobbying the registered political party campaigner to publicly change their policy on Australia's migration policies.