Australian Government
Attorney-General's Department

January 2018

Parliamentary Joint Committee on Intelligence and Security

Attorney-General's Department Submission

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

Contents

Introduction

1. The Attorney-General's Department welcomes the opportunity to provide the Parliamentary Joint Committee on Intelligence and Security with this submission as part of the Committee's inquiry into the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017.

2. The Bill was introduced into the House of Representatives on 7 December 2017 by the Prime Minister, the Hon Malcolm Turnbull MP, and referred to the Committee on 8 December 2017 for inquiry and report by February 2018.

Background

3. On 12 May 2017 the Prime Minister requested that the then Attorney-General, Senator the Hon George Brandis QC undertake a review of Australia's espionage and foreign interference legislation, to consider:

- the adequacy and effectiveness of existing espionage and treason offences under the *Criminal Code Act 1995* (Cth) (Criminal Code), and the official secrets offences under the *Crimes Act 1914* (Cth) (Crimes Act)
- the merit of creating specific foreign interference offences within the Criminal Code
- the merit of creating a legislative regime based on the United States' *Foreign Agents Registration Act 1938*, and
- whether there are any complementary provisions that would strengthen agencies' ability to investigate and prosecute acts of espionage and foreign interference.

4. It was apparent to the review that foreign intelligence services are currently seeking to harm Australia's interests on an unprecedented scale and through a variety of means, including by obtaining classified information or by seeking to influence the outcome of Australia's democratic and institutional processes. The review found that existing criminal offences have proven inadequate in addressing such conduct and have therefore had limited impact in deterring and countering espionage and foreign interference activities occurring in Australia.

Overview of legislative package

5. On 7 December 2017 the Prime Minister introduced a comprehensive package of legislative reforms in response to the Attorney-General's review, including:

- the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017
- the Foreign Influence Transparency Scheme Bill 2017, and

- the Foreign Influence Transparency Scheme (Charges Imposition) Bill 2017.

6. The National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 will amend the Criminal Code, the Crimes Act and the *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA Act). The purpose of the Bill is to modernise and strengthen espionage, treason, secrecy and related criminal offences, and to create new foreign interference offences to ensure the protection of Australia and Australia's national security interests.

7. The Foreign Influence Transparency Scheme Bill 2017 will establish the Foreign Influence Transparency Scheme. The scheme will introduce registration obligations for persons and entities who have certain arrangements with, or undertake certain activities on behalf of, foreign principals. The scheme provides visibility of the nature and extent of foreign influence over Australia's government and political processes.

8. The Foreign Influence Transparency Scheme (Charges Imposition) Bill 2017 will provide legislative authority for the Government to impose charges for applications for registration and renewal of registration under the scheme. Charges are intended to partially offset the costs involved in establishing, administering and maintaining the scheme.

9. In addition to these legislative reforms, the Minister for Finance introduced the Electoral Legislation Amendment Act (Electoral Funding and Disclosure Reform) Bill 2017, which amends the *Commonwealth Electoral Act 1918* (Cth) to improve the consistency of regulations that apply to the financed election campaigns of key political actors. The bill will restrict the ability of foreign money to finance domestic election campaigns by prohibiting donations from foreign governments and state-owned enterprises and will further prohibit political actors from using donations from foreign sources to fund reportable political expenditure.

10. The legislative package represents a comprehensive, whole-of-government effort to address the threat of espionage, foreign interference and foreign influence in Australia.

Overview of submission

11. The submission provides an overview of the nature and extent of the threat of espionage and foreign interference in Australia and the challenges facing law enforcement and national security agencies in addressing this threat.

12. The submission then examines key elements of the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017, including offences for:

- espionage and theft of trade secrets
- foreign interference
- secrecy
- sabotage

- treason, treachery and other threats to security, and
- false or misleading information.

13. The submission also outlines amendments to the TIA Act, which will enable law enforcement and national security agencies to access telecommunications interception powers to investigate the offences included in the Bill.

14. Finally, the submission outlines a number of legislative safeguards in the Bill, which ensure that the offences balance the protection of Australia's national security with the protection of individual rights and freedoms.

Challenges faced by law enforcement and national security agencies

15. Australia's law enforcement and national security agencies face significant challenges in addressing foreign interference and related activities in Australia. A key challenge is the lack of criminal offences for acts of foreign interference, and ineffective criminal offences for related conduct. The absence of effective law enforcement options, and related transparency measures, inhibits the ability of relevant agencies to both deter and disrupt such activity. .

The current threat environment

16. Espionage and foreign interference activities directed at Australian interests are not a new phenomenon; such activity is an enduring feature of the Australian security environment and can cause grave harm to Australia's interests. It can include physical or other harm to individuals, loss of military advantage or compromise of national defences, and economic harm to Australian businesses and national economic well-being more broadly. Interference in Australian political processes seeking to advance the national interest of a foreign nation can undermine Australia's constitutional system of government and national sovereignty.

17. The Australian Security Intelligence Organisation (ASIO) has recently advised that foreign intelligence activities, directed against Australia and Australia's interests, are occurring on an unprecedented scale.[1] ASIO judges that the threat is 'extensive, unrelenting and increasingly sophisticated'.[2]

18. According to ASIO's 2016-2017 Annual Report:

> In addition to traditional espionage efforts to penetrate government, foreign intelligence services are targeting a range of Australian interests, including clandestine acquisition of intellectual property, science and technology, and commercially sensitive information. Foreign intelligence services are also using a wider range of techniques to obtain intelligence and clandestinely interfere in Australia's affairs, notably including covert influence operations in addition to the tried and tested human-enabled collection, technical collection, and exploitation of the Internet and information technology.[3]

19. Furthermore, ASIO has identified an increasing number of states 'clandestinely seeking to shape the opinions of members of the Australian public, media organisations and government officials in order to advance their country's own political objectives.'[4] Ethnic and religious communities are particularly vulnerable to covert influence operations designed to subdue their criticism of foreign governments.[5] Recent domestic media coverage has alleged foreign influence in Australia's political processes. Global events, such as cyber operations

---

[1] Australian Security Intelligence Organisation, *Annual Report 2016-2017*, p45 ('*ASIO Annual Report 2016-2017*').
[2] Ibid, p23.
[3] Ibid, p45.
[4] Ibid, p5.
[5] Ibid.

and reported disinformation campaigns intended to influence the Brexit Referendum, the US election in 2016 and the French and UK elections in 2017, have brought the threat of foreign interference into sharper focus and have highlighted the global nature of the issue.

Outdated and ineffective laws

20. Existing criminal offences have proven to be inadequate and have had limited impact deterring and countering espionage and foreign interference activities occurring in Australia. 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, new vectors to access sensitive data and tools to obscure identity. Many of the existing criminal offences also contain ambiguous or archaic language making the offences extremely difficult to prosecute. A lack of serious criminal penalties for the current offences undermines agencies' efforts to identify, deter and disrupt interference activity in Australia and create an environment that discourages such conduct.

21. In addition to the inadequacy of existing offences, Commonwealth criminal law does not adequately capture foreign interference activities that fall short of the traditional offences of espionage and secrecy. Australia lags behind other jurisdictions such as the United States, Canada and New Zealand which have specific offences targeting foreign interference[6] and economic espionage[7] in addition to more serious secrecy offences.[8]

22. In light of the unprecedented threat environment and the challenges faced by law enforcement and national security agencies, it is essential to expand the scope of the criminal law to cover the diverse range of espionage and foreign interference activities currently occurring in Australia. It is essential that Commonwealth criminal offences cover contemporary methodologies used to carry out such activities as well as capturing those methodologies that may be developed in the future.

23. It is also essential that the full suite of law enforcement powers are available to investigative agencies in order to successfully investigate and prosecute acts of espionage, foreign interference and related threats to Australia's national security as part of a broader whole-of-government response to this issue.

---

[6] 18 USC § 951.
[7] *Economic Espionage Act 1996*, 18 USC §§ 1834-1832; *Security of Information Act,* RSC 1985, c. O-5, s 19; *Crimes Act 1961* (NZ) s 230.
[8] Title 18 USC §§ 793-798; 1924; Title 50 USC § 793; for information on the offences under international regimes see Appendix B.

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

Overview

24. The National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 will comprehensively reform key offences dealing with threats to Australia's national security, particularly those posed by foreign principals. The Bill will:

- strengthen existing espionage offences and introduce a new theft of trade secrets offence to protect Australia from economic espionage
- introduce 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
- reform Commonwealth secrecy offences, ensuring they appropriately criminalise unauthorised disclosures of harmful information while also protecting freedom of speech
- introduce comprehensive new sabotage offences that effectively protect critical infrastructure in the modern environment
- modernise and reform offences against government, including treason, to better protect Australia's defence and democracy
- introduce a new aggravated offence for providing false and misleading information in the context of security clearance processes, and
- ensure law enforcement agencies have access to telecommunications interception powers to investigate these serious offences.

Espionage and theft of trade secrets

25. Espionage is criminalised in Division 91 of the Criminal Code.[9] The offences in Division 91 apply where a person communicates information, or makes, obtains or copies a record, concerning the Commonwealth's security or defence or information acquired from the Commonwealth about the security or defence of another country, with an intention to prejudice the Commonwealth's security or defence or (without lawful authority) to advantage the security or defence of a foreign country.[10] In relation to the communication of information, the offences

[9] *Criminal Code Act 1995* (Cth).
[10] Ibid s 91.1.

apply where the information is, or is likely to be, communicated to another country or a foreign organisation.[11] The offences are punishable by a maximum penalty of 25 years imprisonment.

The need for reform

26. The espionage offences in Division 91 of the Criminal Code are problematic for a number of reasons. First, the offences only apply where a person *intends* to prejudice the security or defence of Australia or to advantage the security or defence of a foreign country. Limiting the application of the offences to situations where the fault element of intention can be proved does not recognise the significant harm that may result from acts of espionage in circumstances where a person engages in the conduct *reckless* as to whether the conduct will prejudice Australia's security or defence or advantage the security or defence of a foreign country.

27. In addition, the evidence required to establish the element of intention is, in many cases, highly sensitive and/or classified and as a result may not be revealed in court, even with the protections provided for by the *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth) (NSI Act). This makes the current offences extremely difficult to prosecute, even when the relevant intention is present.

28. Existing espionage offences are also limited to dealings with information relevant to security or defence. This fails to recognise that dealings with a broader range of information may also result in significant harm to Australia's interests. Under Division 91, the information communicated, or the record made, obtained or copied, must concern the security or defence of Australia or of a foreign country. The definition of 'security and defence of a country' includes the operations, capabilities and technologies of, and methods and sources used by, the country's intelligence or security agencies.[12] Although the disclosure of information which concerns security or defence represents the most serious end of the offending spectrum the communication of information which does not relate to security or defence can be equally damaging, particularly where it is communicated by a person intending to prejudice Australia's interests.

29. For example, the disclosure of sensitive information relating to Australia's foreign policy may be particularly damaging to Australia's diplomatic interests and alliance relationships, but is not necessarily covered by existing espionage offences. Similarly, disclosures of other privileged information held outside the Commonwealth such as information held by private contractors, academic institutions or political organisations, may be as harmful to Australia's national security as information held by the Commonwealth. Existing espionage offences also fail to provide for information which is of significant economic value such as information held by the CSIRO, commercial secrets including Australia's negotiating position on natural gas and iron ore prices as well as trade secrets related to nuclear power, metal, solar production and defence industries, information which has the potential to seriously damage Australia's economic interests.

[11] Ibid s 91.1(1)(c)-(2)(c).
[12] Ibid s 90.1(1).

30. A further difficulty in the prosecution of existing espionage offences is the element of 'lawful authority' which applies where a person communicates information, or makes, obtains or copies a record, intending to advantage the security or defence of a foreign country. This element requires the prosecution to prove, beyond a reasonable doubt, that the there was no authority in any law or in any aspects of the person's duties that authorised the person to deal with the information in the relevant manner. This is a significant barrier to prosecution, especially in circumstances where a malicious insider, with various authorities by virtue of their employment, releases information to a foreign principal.

31. Finally, existing espionage offences have not evolved 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 a wide range of tools to obscure identity. According to the ASIO Annual Report 2016-2017 cyber espionage is on the rise and as technology continues to evolve so too does the sophistication and complexity of cyber-attacks.[13] Furthermore, current Division 91 offences which are limited to conduct which 'communicates information' or 'makes, obtains or copies a record', does not recognise the full range of conduct which may result in the disclosure of harmful information to a foreign country or otherwise prejudice Australia's national security or defence.

32. It is important for Australia's national interest that espionage offences cover the full range of harmful information as well as account for contemporary methodologies used to carry out acts of espionage or those methodologies that may be developed in the future.

Outline of new espionage offences

33. The Bill amends Division 91 and introduces Division 92A into the Criminal Code to include comprehensive new espionage offences, including:

- espionage (*information concerning national security*) – dealing with information that has a security classification or concerns national security, which is or will be *made available to a foreign principal*:
    - with an *intention* to prejudice Australia's national security or advantage the national security of a foreign country (penalty: life imprisonment)
    - *reckless* as to whether the conduct will prejudice Australia's national security or advantage the national security of a foreign country (penalty: 25 years imprisonment)[14]
- espionage – dealing with information which is or will be *made available to foreign principal*:

[13] *ASIO Annual Report 2016-2017,* above n 1, p5.
[14] The National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 (Cth) sch 1 part 1 s 91.1.

- with an *intention* to prejudice Australia's national security (penalty: 25 years imprisonment)

- *reckless* as to whether the conduct will prejudice Australia's national security (penalty: 20 years imprisonment)[15]

- espionage – dealing with information that has a *security classification* or concerns *national security*, which is or will be *made available to a foreign principal* (penalty: 20 years imprisonment)[16]

- espionage on behalf of foreign principal – dealing with information*, on behalf of a foreign principal*, reckless as to whether the conduct *involves the commission of an espionage offence*:

  - with an *intention* to prejudice Australia's national security or advantage the national security of a foreign country (penalty: 25 years imprisonment)

  - *reckless* as to whether the conduct will prejudice Australia's national security or advantage the national security of a foreign country (penalty: 20 years imprisonment)[17]

- espionage on behalf of foreign principal – dealing with information *on behalf of a foreign principal*, reckless as to whether the conduct *involves the commission of an espionage offence* (penalty: 15 years imprisonment)[18]

- aggravated espionage – dealing with information that has a security classification of *SECRET or above*; is from a *foreign intelligence agency*; *involves five or more records*, each of which has a *security classification* or where the person alters a record to *remove or conceal its security classification* or deals within information while *holding an Australian Government security clearance* (penalty: life imprisonment if the underlying offence is 25 years imprisonment, or 25 years imprisonment if the underlying offence is 20 years imprisonment)[19]

- soliciting or procuring an espionage offence – 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* in a way that would *constitute an espionage offence* (penalty: 15 years imprisonment)[20]

---

[15] Ibid, s 91.2.
[16] Ibid, s91.3.
[17] Ibid, s 91.8(1)-(2).
[18] Ibid, s 91.8(3).
[19] Ibid, s 91.6.
[20] Ibid, s 91.11.

- preparing for an espionage offence – conduct in *preparation for*, or *planning*, an offence of *espionage*, or espionage on behalf of a foreign principal (penalty: 15 years imprisonment)[21]

- theft of trade secrets (economic espionage) – *dishonestly* receiving, obtaining, taking, copying or duplicating, selling, buying or disclosing information that is a *trade secret* on behalf of a *foreign government principal* (penalty: 15 years imprisonment).[22]

34. New espionage offences will apply tiered penalties ranging from 15 years to life imprisonment. The tiered penalties will ensure that the penalty for each offence is commensurate with the seriousness of the offence and culpability of the offender. The lower penalty of 15 years imprisonment will apply to espionage-related offences such as soliciting or procuring a person to engage in espionage or preparing or planning for an espionage offence. The highest penalty of life imprisonment will apply to the most egregious conduct, which involves dealing with security classified information or information relevant to national security with an intent to prejudice Australia's national security or advantage the national security of a foreign country, resulting in the information being made available to a foreign principal.

35. The maximum penalty of life imprisonment is significantly higher than the maximum penalty of 25 years imprisonment for existing espionage offences. The purpose of increasing the penalty is to ensure that it appropriately reflects the gravity of the offence. Less serious conduct will be criminalised in separate offences and subject to lower penalties. This ensures that the most serious penalty of life imprisonment is only available in circumstances representing the worst possible category of offending.

36. Increasing penalties of imprisonment in these circumstances is consistent with the established principles of Commonwealth criminal law policy as set out in the Guide to Framing Commonwealth Offences[23] to impose a heavier penalty where the consequences of the offence are particularly dangerous or damaging. Increasing penalties of imprisonment will also contribute to deterrence of the commission of espionage offences.

37. For information on the penalty for each espionage offence see **Appendix C**.

Key changes to espionage offences

38. The key changes to espionage offences include:

- the criminalisation of a broader range of dealings with information

- the protection of a broader range of information

---

[21] Ibid, s 91.12.
[22] Ibid, s 92A.1.
[23] Available at https://www.ag.gov.au/Publications/Pages/GuidetoFramingCommonwealthOffencesInfringementNoticesandEnforcementPowers.aspx

- the introduction of offences of espionage on behalf of a foreign principal
- the introduction of offences applying recklessness as the fault element, rather than intention
- the inclusion of lawful authority as a defence
- the introduction of an aggravated espionage offence
- the introduction of an offence of soliciting or procuring a person to engage in espionage
- the introduction of an offence to prepare or plan for an espionage offence
- the introduction of an offence targeting the theft of trade secrets (economic espionage).

Dealings with information

39. New espionage offences will criminalise conduct which 'deals with' information, rather than being limited to the 'communication of information.' A person 'deals with' information if the person receives or obtains; collects; possesses; makes a record of; copies; alters; conceals; communicates; publishes or otherwise makes the information available.[24] By broadening the offences to cover conduct which 'deals with' information, the new offences will capture the full range of conduct undertaken by foreign adversaries seeking to compromise sensitive information and prejudice Australia's national security.

40. For example, the Bill includes the terms possess, alters, conceals and receives in the definition of 'deals'. These are not currently covered by the espionage offences in Division 91 of the Criminal Code. Covering these activities is important, as this conduct can be damaging in itself as well as part of a course of conduct leading up to a disclosure.

Types of information

41. The new espionage offences will apply to:

- information which is security classified or which concerns Australia's national security (section 91.1), and
- all information (section 91.2).

42. The definition of security classified information will be prescribed in regulations. It is anticipated that the regulations will prescribe the relevant protective markings that will denote information as being classified for the purpose of the offences. These markings are currently listed in the *Australian Government information security management*

[24] Ibid, s 90.1(1).

guidelines – Australian Government security classification system and include PROTECTED, CONFIDENTIAL, SECRET and TOP SECRET.

43. The definition of Australia's national security will include:

- 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 including espionage, sabotage, terrorism, political violence, foreign interference and activities intended to interfere with the performance of the country's defence force
- 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 including espionage, sabotage, terrorism, political violence, foreign interference and activities intended to interfere with the performance of the country's defence force, and
- the country's political, military or economic relations with another country or other countries.[25]

44. The definition of national security expands the definition of 'security and defence' provided by existing espionage offences, to more comprehensively cover the matters relevant to the security of a country. As a result new espionage offences will protect a broader range of information in order to address the fact that foreign actors seek access to all types of information.

45. In relation to the offences in section 91.2 (which apply to all information), the methodology of Australia's adversaries means that even dealings with unclassified information or publicly available information can be equally as damaging to Australia's national security interests as dealings with classified information. This is particularly so when it is done with the intention to prejudice Australia's national security or where a person is reckless as to whether their conduct will prejudice Australia's national security. The offences in section 91.2 will only apply where a person intends to, or is reckless as to whether their conduct will prejudice Australia's national security and not where a person seeks to advantage the national security of a foreign principal.

Espionage on behalf of a foreign principal

46. The Bill will introduce specific espionage offences which apply where a person engages in conduct on behalf of, or directed, funded or supervised by, a foreign principal

[25] Ibid, s 90.4.

or a person acting on behalf of a foreign principal.[26] The introduction of these offences recognises the serious consequences that may result from acts of espionage undertaken on behalf of a foreign principal, which seriously undermines Australia's sovereignty and national security.

47. The offences will apply tiered penalties ranging from 10 to 25 years imprisonment and will depend upon the seriousness of the offence and the culpability of the offender. Where an offence on behalf of a foreign principal is committed with an intention to prejudice Australia's national security or advantage the national security of a foreign country, a maximum penalty of 25 years imprisonment applies. This penalty is appropriate to deter and punish a worst case offence which may result in 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.

Recklessness offences

48. New espionage offences will implement a tiered approach, covering both intentional and reckless conduct. The introduction of offences for recklessness addresses the significant harm that may result from acts of espionage in circumstances in which a person lacks the relevant intent but nevertheless engages in the conduct, reckless as to the relevant circumstances or result. They are designed to capture the full range of conduct undertaken by foreign intelligence services and other malicious actors seeking to compromise information and prejudice Australia's national security.

49. Under section 5.4 of the Criminal Code, the fault element of recklessness provides that a person is reckless with respect to a circumstance or a result if he or she is aware of a substantial risk that the circumstances exists or will exist or the result will occur and having regard to the circumstances known to him or her, it is unjustifiable to take the risk.[27]

50. The benefit of adding offences that have recklessness as a fault element is that it provides a range of options to law enforcement and prosecutorial agencies when investigating espionage offences. It also allows for tiered penalties to be applied, with the highest penalties applying to the most serious offences where intention is established, and lower penalties applying where recklessness is established.

Lawful authority as a defence

51. Espionage offences 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

[26] Ibid, s 91.8.
[27] Criminal Code, s5.4.

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 communicating information concerning national security is a daily requirement in many Commonwealth departments and agencies and for Ministers and their staff. Espionage offences are not intended to criminalise these dealings.

52. 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. This element requires the prosecution to prove that the person did not have lawful authority for their actions, which is extremely difficult to prove beyond a reasonable doubt.

53. New espionage offences cast the matter of lawful authority as a defence. The defence will apply to espionage and espionage related offences where a person deals with information:

- in accordance with a law of the Commonwealth
- in accordance with an arrangement or agreement to which the Commonwealth is party and which allows for the exchange of information or articles, or
- in the person's capacity as a public official.[28]

54. By introducing lawful authority as a defence, the evidentiary burden of proof will be transferred to the defendant.[29] This is appropriate because the source of the alleged authority for the defendant's actions is peculiarly within the defendant's knowledge and as such the defendant should be readily able to point to evidence that they had lawful authority, for example that their duties authorised them to deal with the information or thing in the relevant manner. It is more appropriate for the defendant to assert this matter rather than the prosecution needing to disprove the existence of any authority. Imposing a burden on the defendant in these circumstances is consistent with the Guide to Framing Commonwealth Offences.

Aggravated espionage

55. An aggravated espionage offence will apply where a person deals with information that has a security classification of SECRET or above; is from a foreign intelligence agency; involves five or more records, each of which has a security classification or where the person alters a record to remove or conceal its security classification or deals

[28] Sections 91.4, 91.9, 91.13
[29] In the case of an evidential burden of proof, the defendant bears the burden of adducing or pointing to evidence that suggests a reasonable possibility that the matter exists or does not exist (Criminal Code section 13.3). If the defendant discharges an evidential burden, the prosecution must disprove these matters beyond a reasonable doubt consistent with section 13.1 of the Criminal Code.

within information while holding an Australian Government security clearance.[30] However, the aggravated offence will not apply where a person has a defence to the underlying espionage offence.

56. 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. Where the underlying offence carries a maximum penalty of life imprisonment, the aggravating conduct will be taken into account by a court in determining the sentence to be imposed, in accordance with section 91.5 of the Bill.

57. The introduction an aggravated espionage offence reflects the higher level of culpability associated with dealing with information in the circumstances described above; as such conduct poses an extreme risk to Australia's national security. 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 higher penalty where the consequences of an offence are particularly dangerous or damaging.

Soliciting or procuring an espionage offence

58. The Bill will make it an offence to engage in conduct in relation to another person, with the intention of soliciting or procuring, or making it easier to solicit or procure that person to deal with information in a way that would constitute an espionage offence.[31] The purpose of this offence is to address gaps in the current law, which does not criminalise soliciting or procuring espionage. This offence will enable foreign actors who task others to undertake espionage activities against Australian interests to be charged and prosecuted under Australian law. The offence will further enable law enforcement to deal with the 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.

59. The maximum penalty for the offence is 15 years imprisonment. This penalty reflects the serious harm that can flow from activities which seek to solicit or procure a person to engage in espionage, especially if a foreign principal is successful in obtaining classified information that will prejudice Australia's national security.

60. The penalty 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.

[30] Section 91.6
[31] Section 91.11

Preparing or planning for an espionage offence

61. The Bill will introduce an offence for preparing for or planning 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.[32] This is similar to preparatory offences enacted in relation to terrorism[33] and child sex offences.[34]

62. 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 an espionage offence is committed or sensitive information is actually passed to a foreign principal.

63. 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, this offence 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.

Theft of trade secrets (economic espionage)

64. The Bill will introduce new Division 92A into the Criminal Code which will contain an offence criminalising the theft of trade secrets on behalf of a foreign government principal.[35] The purpose of this offence is to combat the increasing threat of data theft, business interruption and economic espionage, particularly by or on behalf of foreign individuals and entities. Interference in Australia's commercial dealings and trade relations by or on behalf of foreign governments has serious consequences for Australia's national security and economic interests. Examples of targets for economic espionage in Australia might include highly valuable and sensitive information held by the CSIRO and the Defence Science and Technology Group, commercial secrets such as negotiating position on natural gas and iron ore prices and trade secrets related to nuclear power, metal, solar production and defence industries (including trade secrets held by private contractors).

65. The new offence will apply where a person dishonestly receives, obtains, takes, copies or duplicates, sells, buys or discloses information that is a trade secret on behalf of a foreign government principal. Information will constitute a 'trade secret' where:

- the information was not generally known in trade or business, or in the particular trade or business concerned,

[32] Section 91.12
[33] Section 101.6 of the Criminal Code.
[34] Sections 272.20 and 474.25C of the Criminal Code.
[35] Subsection 92A.1(1)

- the information had an economic value, or a higher economic value than it otherwise would have, because it was not known in trade or business or the trade or business concerned, and

- the owner of the information had made reasonable efforts in the circumstances to prevent that information from becoming generally known.

66. The circumstances in which information will constitute a trade secret are consistent with other international regimes which criminalise the theft of trade secrets. More information on relevant international offences is at **Appendix B**.

Foreign interference

The need for foreign interference offences

67. Australia's foreign adversaries do not rely solely on espionage in order to pursue their objectives. Foreign actors and intelligence services are increasingly engaged in a variety of foreign interference activities relating to Australia. These activities are directed against a range of Australian interests, including Australia's political systems, military capabilities and commercial pursuits.

68. 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 objectives. Foreign interference goes beyond 'soft power', as the term is properly understood – as an attractive force where a nation exerts a cultural or economic gravitational pull influencing another country.

69. ASIO has advised that foreign intelligence activities directed against Australia are occurring on an unprecedented scale. This is not only occurring in relation to Australia – similar increased threat has been identified in other countries. Recent events overseas, including cyber operations and disinformation campaigns designed to manipulate foreign elections and other democratic decision making processes, further highlight the significance of the threat of foreign interference.

70. In Australia, there are currently no criminal offences targeting foreign interference. The lack of criminal offences for this type of conduct has resulted in a permissive operating environment for malicious foreign actors, which Australian agencies are unable to effectively disrupt and mitigate. To address this gap, the Bill will introduce Division 92 into the Criminal Code which will contain new foreign interference offences. These offences will complement 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.

Outline of foreign interference offences

71. New Division 92 will contain the following foreign interference offences:

- Intentional foreign interference (interference generally) – *covert, deceptive, threatening or menacing conduct* engaged in *on behalf of a foreign principal*, with an *intention to influence* a political or governmental process of the Commonwealth or a State or Territory or the exercise of an Australian democratic or political right, *support intelligence activities* for a foreign principal or *cause harm* to Australia's national security (penalty: 20 years imprisonment)[36]

- Intentional foreign interference (interference involving targeted person) – *conduct* engaged in *on behalf of a foreign principal*, with an *intention to influence another person* (the target) in relation to a political or governmental process of the Commonwealth or a State or Territory or the target's exercise of an Australian democratic or political right or duty, and the *relationship with the foreign principal is not disclosed* to the target (penalty: 20 years imprisonment)[37]

- Reckless foreign interference (interference generally) – *covert, deceptive, threatening or menacing conduct*, engaged in *on behalf of a foreign principal*, *reckless* as to whether the conduct will *influence* a political or governmental process of the Commonwealth or a State or Territory or the exercise of an Australian democratic or political right, *support intelligence activities* for a foreign principal or *cause harm* to Australia's national security (penalty: 15 years imprisonment)[38]

- Reckless foreign interference (interference involving targeted person) – *conduct engaged in on behalf of a foreign principal*, *reckless* as to whether the conduct will *influence another person* (the target) in relation to a political or governmental process of the Commonwealth or a State or Territory or the target's exercise of an Australian democratic or political right or duty, and the *relationship with the foreign principal is not disclosed* to the target (penalty: 15 years imprisonment)[39]

- Preparing for a foreign interference offence – conduct in *preparation for*, or *planning*, an *foreign interference offence* (penalty: 10 years imprisonment)[40]

[36] Subsection 92.2(1)
[37] Subsection 92.2(2)
[38] Subsection 92.3(1)
[39] Subsection 92.3(2)
[40] Section 92.4

- Knowingly supporting a foreign intelligence agency – providing *support* or resources to an organisation *knowing* that the organisation is a *foreign intelligence agency* (penalty: 15 years imprisonment)[41]

- Recklessly supporting a foreign intelligence agency – providing *support* or resources to an organisation *reckless* as to whether the organisation is a *foreign intelligence agency* (penalty: 10 years imprisonment)[42]

- Knowingly funding or being funded by a foreign intelligence agency – *receiving or obtaining funds from or collecting funds on behalf of* an organisation, *knowing* that the organisation is a *foreign intelligence agency* (penalty: 15 years imprisonment)[43]

- Recklessly funding or being funded by a foreign intelligence agency – *receiving or obtaining funds from or collecting funds on behalf of an* organisation, *reckless* as to whether the organisation is a *foreign intelligence agency* (penalty: 10 years imprisonment)[44]

72. The foreign interference offences attract tiered penalties ranging from 10 to 20 years imprisonment. This approach ensures that the penalty for each offence is commensurate with the seriousness and culpability of offending. Higher penalties will apply where the offence is committed with an intent to influence a political or governmental process or democratic or political right, support intelligence activities of a foreign principal or prejudice Australia's national security. A summary of the penalties for each foreign interference offence is at **Appendix D**.

73. A defence will apply to foreign interference offences where a person engages in conduct:

- in accordance with a law of the Commonwealth

- in accordance with an arrangement or agreement to which the Commonwealth is party and which allows for the exchange of information or articles, or

- in the person's capacity as a public official.[45]

74. The defence applies where a person engages in conduct covered by the foreign interference offences in the performance of the person's duties as a public official. Many departments and agencies engage in joint activities with international counterparts as part of their normal business dealings. Foreign interference offences are only intended to apply where a person's conduct is not a proper or legitimate part of their work. It will not

[41] Section 92.7
[42] Section 92.8
[43] Section 92.9
[44] Section 92.10
[45] Sections 92.5 & 92.11

be a defence to a charge of foreign interference where a person has gone beyond their proper duties.

Examples of foreign interference

75. Examples of conduct that would fall within the scope of the new foreign interference offences include:

- An Australian citizen who works for a national security agency, provides sensitive information to foreign officials, at their direction and in exchange for cash and benefits. The Australian citizen uses tradecraft to conceal this relationship and the passage of unclassified (but produced by Government) information from Australian authorities. This concealment also occurs during interviews for the yearly re-evaluation of the appropriateness of the Australian citizen holding a top secret security clearance.

- An individual in Australia receives and acts upon intelligence tasking from a foreign intelligence service. Tasking includes requests for financial information, facilitation of meetings with politicians, and access to unclassified government information about sanctions on the foreign country. Meetings between the individual and an undeclared officer are held secretly, with tradecraft used to conceal meeting arrangements and content.

- A person in Australia monitors dissidents in Australia and passes the information to a foreign intelligence service which uses this information to harass and intimidate the dissidents and their relatives. The Australia-based person conceals the purpose of their travel to the foreign country and engagement with foreign intelligence officials from Australian authorities when asked at the airport.

- In response to direction from a foreign diplomat, an Australian citizen lobbies senior Australian decision-makers and conducts public advocacy activities in support of the strategic interests of the foreign country. The Australian citizen does not disclose this foreign diplomat relationship while conducting these lobbying activities, and receives significant preferential treatment in that foreign country.

- An Australian citizen academic is in an undisclosed, witting and ongoing relationship with a foreign official in Australia. The foreign official provides the Australian citizen with disinformation suggesting a major Australian business has engaged in foreign bribery activities, and tasks the Australian citizen to circulate this information to media, political and official contacts. While not directly affecting governmental or political processes, this disinformation is intended to attract public attention and prejudice the interests of the Australian business.

- An Australian citizen is a decision-maker in a political organisation, in an undisclosed, witting and ongoing relationship with a foreign official in Australia. The foreign official asks the Australian citizen to consistently criticise an alliance partner and promote the alternative foreign country relationship within the political organisation, in order to undermine the alliance partner's confidence in the political organisation. While not directly affecting an Australian governmental or political process, this activity is intended to undermine Australia's national interests (i.e. the alliance).

76. The following conduct would fall within the scope of the preparatory offences for foreign interference:

- An Australian citizen is in an ongoing relationship with an individual they know to be an overseas-based foreign intelligence service (FIS) officer. In response to specific requests from the FIS officer, the Australian subscribes multiple mobile telephones and books accommodation under their own name, to provide directly to the FIS officer travelling to Australia. The Australian citizen is aware these items are for the use of the FIS officer in Australia, but does not declare this to the telephone companies, hotel operators or Australian authorities. The Australian citizen believes the FIS office is travelling for operational purposes, but does not know the specifics. The Australian citizen also attends dissident group meetings in Australia and provides lists of attendees to the FIS officer. The Australian citizen believes the FIS officer will use this information for threatening purposes, but is unaware of the specifics. The Australian citizen does not disclose the FIS officer request to any of the attendees or Australian authorities when asked. The FIS officer subsequently fails to travel, or does not threaten the dissidents, despite having the items and information provided by the Australian citizen.

- A FIS directs a foreign company to acquire strategic business premises located in close proximity to Australian critical infrastructure, with the intention that this acquisition could provide the FIS access to valuable intelligence information in the future.

77. The foreign interference offences were informed by the offence of 'agents of foreign governments' in the US Code.[46] The proposed offences do not however include an element of 'without prior notification to the Attorney-General', as the intention of the foreign interference offences is to capture conduct that is always criminal, and that cannot be excused by 'notification' to a public official.

78. The foreign interference offences were also informed by the definition of 'acts of foreign interference' in section 4 of the *Australian Security Intelligence Organisation Act 1979*, which defines this term for the purposes of ASIO's intelligence functions. The

[46] 18 USC 951

proposed provisions draw on and adopt the definition to develop provisions appropriate in the context of criminal offences.

Secrecy

79. Secrecy offences are an essential part of Commonwealth criminal law. Such offences protect privileged and classified information from being inappropriately disclosed. It is essential for Australia to safeguard such information, including to protect it from being improperly obtained by foreign intelligence services or other malicious actors. The inappropriate disclosure of privileged or classified information could place Australians in danger of grave harm. It could also damage Australia's essential national interests by, for example, damaging Australia's international relations or interfering with criminal investigations.

80. In its 2009 report titled *Secrecy Laws and Open Government in Australia (Report 112)*, the Australian Law Reform Commission undertook a mapping exercise which identified 506 secrecy provisions in 1765 pieces of primary and subordinate Commonwealth legislation. Approximately 70% of these provisions created criminal offences.

81. In addition to these specific secrecy offences, Parts VI and VII of the Crimes Act contain secrecy offences of general application.

- Section 70 applies criminal penalties to the unauthorised disclosure of facts or documents by current and former Commonwealth officers who are under a duty not to disclose the fact or document, and is punishable by two years' imprisonment.

- Section 79 covers unauthorised disclosure as well as certain other conduct, and applies to persons other than Commonwealth officers:

    - Subsection 79(2) prohibits an unauthorised communication, retention or failure to comply with a lawful direction of information, when done with the intention to prejudice security or defence, and is punishable by seven years' imprisonment.

    - Subsection 79(3) prohibits the unauthorised communication of information and is punishable by two years' imprisonment. This differs from section 70 in its application to non-Commonwealth officers, and its extension to 'making available' information (in addition to communicating or publishing that information).

    - Subsection 79(4) prohibits the unauthorised retention, failure to comply with a direction, or failure to take reasonable care (etc) of information, and is punishable by six months' imprisonment.

    - Subsection 79(5) prohibits receipt of information if the person knows or has reasonable grounds to believe that it is communicated in contravention of

section 91.1 of the Criminal Code (espionage) or subsection 79(2). This offence is punishable by seven years' imprisonment.

- Subsection 79(6) prohibits receipt of information if the person knows or has reasonable grounds to believe that it is communicated in contravention of subsection 79(3). This offence is punishable by two years' imprisonment.

- The offences in subsections 79(5) and (6) do not apply if the defendant proves that the communication was 'contrary to his or her desire'.

- Section 83 prohibits making, recording, possessing or communicating 'unlawful soundings'[47] and is punishable by two years' imprisonment. The defendant bears the onus of proving that any soundings were not unlawful. All soundings taken in Australian territorial waters are assumed to be unlawful unless:

  - done with the authority of the Australian Government, a state or territory government, or the Queen

  - were reasonably necessary for the navigation of the vessel from which the soundings were taken, or

  - were reasonably necessary for any purpose in which the vessel from which the soundings were taken was lawfully engaged.

The need for reform

82. There have been calls for significant reforms to the general secrecy offences in the Crimes Act for many years. Most significantly, the 2009 ALRC report, Secrecy Laws and Open Government in Australia (ALRC Report 112), recommended amending the provisions to limit the offence to disclosures that include an element of harm.

83. The current offences are archaic and difficult to prosecute. It is unclear what fault elements attach to which elements of the offence, and whether a successful prosecution under section 79(5) or 79(6) depends on the prosecution's ability to make out all the elements of another person's offence under subsection 79(2) of the Crimes Act or section 91.1 of the Criminal Code. The penalties for the offences are also very low – subsection 79(4) (unlawful retention etc.) has a maximum penalty of only six months' imprisonment. The 'information' covered is also narrow and would not include opinions or advice, for example.

84. In particular, section 70 creates an offence where a person breaches a duty not to disclose information but the section itself does not create such a duty. A person will only

[47] 'Sounding' is not defined in the Crimes Act. The Oxford English Dictionary defines 'sounding' as the action or process of sounding or ascertaining the depth of water, usually by means of an echo, or the determination of any physical property at a depth in the sea or at a height in the atmosphere. Section 83(4) provides that any figure, word or sign representing a figure appearing on any map or sketch of the Australian coast or territorial waters is a record of an unlawful sounding.

commit an offence where a duty can be established elsewhere, for example in the *Public Service Act 1999* or other legislative provisions. It is not clear whether this duty must be established by a law or whether a contractual or equitable duty is sufficient to enliven the offence.

85. The definition of 'Commonwealth officer' is set out in section 3 of the Crimes Act. It means a person holding office under, or employed by, the Commonwealth, and includes persons engaged under the *Public Service Act 1999*, AFP and ADF employees, and persons performing services for or on behalf of the Commonwealth. It is unclear whether ministers and their staff fall within this definition. Unlike the Public Service Act and its supporting regulations, the *Members of Parliament (Staff) Act 1984* contains no clear duty not to disclose information. While there is a provision in the Code of Conduct for Ministerial Staff regarding the appropriate use of information, this only applies to personal and electorate staff of Ministers and Parliamentary Secretaries.

Overview of new secrecy offences

86. The Bill proposes to repeal Parts VI and VII of the Crimes Act and create new secrecy offences in the Criminal Code. The offences will criminalise the communication of information that is inherently harmful or would otherwise cause harm to Australian interests.[48]

- Inherently harmful information is defined in section 121.1 of the Bill to mean information that is:
  - security classified information[49]
  - information the communication of which would, or could reasonably be expected to, damage the security or defence of Australia[50]
  - information that was obtained by, or made by or on behalf of, a domestic intelligence agency[51] or a foreign intelligence agency[52] in connection with the agency's functions

[48] The offence regarding communication of inherently harmful information is at subsection 122.1(1). The offence regarding communication causing harm to Australia's interests is at subsection 122.2(1).
[49] Section 121.1 of the Bill provides that information is security classified if it has a security classification. Section 90.5 provides that 'security classification' has the meaning prescribed by the regulations.
[50] Section 121.1 of the Bill provides that 'security or defence of Australia' includes the operations, capabilities or technologies of, or methods or sources used by, domestic intelligence agencies or foreign intelligence agencies.
[51] Section 121.1 of the Bill provides that 'domestic intelligence agency' means the Australian Secret Intelligence Service, the Australian Security Intelligence Organisation, the Australian Geospatial-Intelligence Organisation, the Defence Intelligence Organisation, the Australian Signals Directorate or the Office of National Assessments.
[52] Item 24 of the Bill inserts a new definition of 'foreign intelligence agency' into the Dictionary to the Criminal Code. 'Foreign intelligence agency' is defined to mean an intelligence or security service (however described) of a foreign country.

- 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, and
- information relating to the operations, capabilities or technologies of, or methods or sources used by, a domestic or foreign law enforcement agency.

- Cause harm to Australian interests is defined in section 121.1 of the Bill to mean to:
  - interfere with or prejudice the prevention, detection, investigation, prosecution or punishment of a criminal offence against, or a contravention of a civil penalty provision of, a law of the Commonwealth
  - interfere with or prejudice the functions of the Australian Federal Police in relation to protective, custodial and proceeds of crime functions
  - harm or prejudice Australia's international relations in relation to information that was communicated in confidence to the Commonwealth by or on behalf of a foreign government
  - harm or prejudice Australia's international relations in any other way
  - harm or prejudice relations between the Commonwealth and a State or Territory, or
  - harm or prejudice the health or safety of the public or a section of the public.

87. The offences for communication of inherently harmful information or communication of information causing harm to Australia's interests carry maximum penalties of 15 years imprisonment.

88. The Bill also creates offences for other dealings with inherently harmful information and other conduct causing harm to Australia's interests.[53] This includes offences for:

- dealing with information (other than by communicating it), for example by copying or concealing information
- removing information from, or holding information outside, a proper place of custody[54] for the information, and
- failing to comply with a lawful direction regarding the retention, use or disposal of information.

[53] See subsections 122.1(2)-(4) and subsections 122.2(2)-(4).
[54] Section 121.2 provides that 'proper place of custody' has the meaning prescribed by the regulations.

89. For the offences to apply, the information must have been made or obtained by a person by reason of his or her being, or having been, a Commonwealth officer[55] or otherwise engaged to perform work for a Commonwealth entity.

90. The offences in sections 122.1 and 122.2 will apply to all persons. Their application will not be limited to Commonwealth officers.

91. The Bill includes an aggravated offence which applies a higher penalty if a person commits an offence against section 122.1 or 122.2 and any 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
- the information is marked with a code word, 'for Australian eyes only' or as prescribed by the regulations
- the underlying offence involves five or more records, each of which has a security classification
- 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.

92. The Bill also includes a modernised version of the existing general secrecy offence in section 70 of the Crimes Act. This new offence (in section 122.4) will apply to current and former Commonwealth officers who communicate information in breach of a duty not to disclose the information, where the duty arises under a law of the Commonwealth.

93. The Bill also includes a number of defences to ensure that the offences do not criminalise appropriate dealings with information or unjustifiably impede freedom of speech or expression. The defendant will bear an evidential burden for these defences.

- Subsection 122.5(1) provides a defence if a person was exercising a power, or performing a function or duty, in the person's capacity as a Commonwealth officer or the person dealt with, removed or held the information in accordance with an arrangement or agreement to which the Commonwealth is a party and which allows for the exchange of information.

[55] 'Commonwealth officer' is defined in section 121.1 of the Bill to mean an APS employee, an individual appointed or 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 Australian Federal Police, an officer or employee of a Commonwealth authority, an individual who is a contracted service provider for a Commonwealth contract, or 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.

- Subsection 122.5(2) provides 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.

- Subsection 122.5(3) provides a defence if the person communicated the information to the Inspector-General of Intelligence and Security, the Commonwealth Ombudsman or the Law Enforcement Integrity Commissioner for the purpose of them exercising a power or performing a function or duty.

- Subsection 122.5(4) provides a defence if the person communicated the information in accordance with the *Public Interest Disclosure Act 2013*.

- Subsection 122.1(5) provides a defence if the person communicated the information to a court or tribunal, whether or not as a result of a requirement.

- Subsection 122.5(6) provides a defence if a person's dealing with, or holding of, information is in the public interest and is in the person's capacity as a journalist engaged in fair and accurate reporting. Subsection 122.5(7) clarifies that it will not be in the public interest if the dealing or holding will, or is likely to, harm or prejudice the health or safety of the public or a section of the public or the dealing or holding would be an offence under:

    - section 92 of the *Australian Security Intelligence Organisation Act 1979*, relating to publication of identity of ASIO employees or ASIO affiliates

    - section 41 of the *Intelligence Services Act 2001*, which relates to publication of identities of intelligence agency staff

    - section 22, 22A or 22B of the *Witness Protection Act 1994*, relating to Commonwealth, Territory, State participants or information about the National Witness Protection Program

- Subsection 122.5(8) provides a defence if there has been a prior publication in certain circumstances, and the person reasonably believes that the communication will not cause harm to Australia's interests or the security or defence of Australia.

- Subsection 122.5(9) provides a defence if a person deals with information that relates to them, or where a person has consented to another person dealing with information that relates to them.

94. The Bill allows courts to grant injunctions under the *Regulatory Powers (Standard Provisions) Act 2014* to restrain a person from contravening the secrecy offences in Division 122 of the Criminal Code. The Bill also provides for articles used in contravention of Part 5.6 of the Criminal Code to be forfeited to the Commonwealth.

95. Category D extended geographical jurisdiction applies to the secrecy offences in Part 5.6. The effect of this is that the offences will apply 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.

Key changes to secrecy offences

Secrecy offences have been modernised

96. Sections 70 and 79 were part of the original Crimes Act, as enacted in 1914.[56] The provisions were repealed and substituted in 1960,[57] when section 70 was extended to cover disclosure by former Commonwealth officers and section 79 was enacted in its current form. Only minor amendments have been made to sections 70 and 79 since that time.

97. Sections 70 and 79 have not been amended to reflect modern drafting styles. They are not consistent with the drafting style of the Criminal Code, which separates each physical element into a separate paragraph, bringing clarity to the physical and fault elements that constitute the offence.

98. The offences do not reflect the contemporary offending being seen in the modern environment. The threats that the offence seeks to target reflect a 1960s mindset about communication of government information. In the modern environment, the threat extends beyond the passage of facts and documents. Government officials and contractors are commonly targeted (by foreign intelligence services and others) to provide informed comment or opinions. Communication of such information, where it is inherently harmful or is likely to cause harm, should be covered by secrecy offences.

99. The Bill repeals Parts VI and VII of the Crimes Act and enacts new, modern secrecy offences in the Criminal Code. The offences have been drafted consistent with modern conventions, ensuring that the physical and fault elements are clear.

Harm based approach and consistency with ALRC recommendations

100. The new primary secrecy offences in the Bill apply where the communication (or other dealing) with information is likely to cause harm. This approach is informed by the Australian Law Reform Commission 2009 inquiry, Secrecy Laws and Open Government in Australia.

101. The ALRC recommended that general secrecy offences should apply to disclosures that are harmful. Recommendation 5-1 states that:

> The general secrecy offence should require that the disclosure of Commonwealth information did, or was reasonably likely to, or intended to:

[56] Act No. 12 of 1914, accessible at https://www.legislation.gov.au/Details/C1914A00012/Download.
[57] Crimes Act 1960, Act No. 84 of 1960, accessible at https://www.legislation.gov.au/Details/C1960A00084

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.

102. In relation to 'inherently harmful information', the Bill departs from the ALRC's recommendations as it protects the categories of information listed in the definition of 'inherently harmful information' at section 121.1. The offence at section 122.1 does not require proof of an express harm requirement, as it is premised on certain categories of information being 'inherently harmful'. The definition of 'inherently harmful information' is exhaustive, and the categories of information covered are necessarily narrow. This includes security classified information and information the communication of which would, or could reasonably be expected to damage the security or defence of Australia.

103. One example where the Bill departs from the ALRC's recommendations is security classified information. The ALRC considered that this should not be a category of information protected by a general secrecy offence due to its view that proof of a harm element should be required. However, disclosure of security classified information is, by its nature, harmful. This category has therefore been included in the definition of 'inherently harmful information'.

104. Information should only be security classified if adverse consequences would result from unauthorised compromise or misuse of the information.[58] 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.

105. In addition to the offence at section 122.1 for 'inherently harmful information', the Bill also contains a general secrecy offence that applies where a person's communication (or other dealing with information) does, will or is likely to cause harm to Australia's interests. This is consistent with the ALRC's recommendations. The Bill defines 'causes harm to Australia's interests' in section 121.1 and limits the definition to serious matters affecting Australia national interests, such as interfering with criminal investigations or

[58] Australian Government Information security management guidelines, accessible at https://www.protectivesecurity.gov.au/informationsecurity/Documents/INFOSECGuidelinesAustralianGovernmentSecurityClassificationSystem.pdf.

harming Australia's international relations. This limits the application of the offence only to serious harms, and ensures the offence does not unreasonably burden freedom of speech.

Duty not to disclose information

106. As set out above in paragraph 80, section 70 of the Crimes Act applies criminal penalties to the unauthorised disclosure of facts or documents by current and former Commonwealth officers who are under a duty not to disclose the facts or documents.

107. The ALRC recommended the repeal of this offence. The Bill instead retains a modernised form of the offence in section 122.4. The new offence applies 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.

108. The reforms in the Bill were developed as part of a review specifically focused on espionage and foreign interference laws. The review considered the important role of general secrecy offences in addressing the continuum of criminal behaviour that can ultimately result in the commission of an espionage offence. It did not comprehensively review all secrecy offences across the statute book.

109. This offence has been included in the Bill because many Acts and Regulations impose duties of non-disclosure on Commonwealth officers that enliven the offence in section 70. If section 70 were repealed without replacement, those duties would lose their criminal enforceability, potentially undermining the protection of information that should be protected.

110. Each specific secrecy offence will need to be considered separately, in the context of the overall legislative framework in which the provision is located. It is proposed that, 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, the offence is not subject to a sunset provision.

Balancing national security concerns with freedom of speech/implied freedom of political communication

111. Secrecy offences are often perceived as draconian and intended to stifle free expression and debate. They can also be perceived as preventing whistle blowing about public sector misconduct or corruption. The ALRC supported the ongoing need for general secrecy offences and noted the challenge of striking the right balance between 'the public interest in open and accountable government and the public interest in maintaining the confidentiality of some government information'.[59]

[59] Paragraph 2.80, *Secrecy Laws and Open Government in Australia* (ALRC Report 112).

112. The Bill strikes an appropriate balance, by criminalising dealings with information that is inherently harmful as well as dealings with information that are likely to cause harm to Australia's interests. These offences are complemented by a modernised offence preventing Commonwealth officers from communicating information that they are under a legal duty not to disclose. The offences are tiered so that the most serious penalties attach to conduct involving communication of inherently harmful information and information that does, will or is reasonably likely to cause harm to Australia's interests.

113. The new secrecy offences in the Bill are not intended to impact on free and open public discussion and debate of issues or information already in the public domain. The Bill contains defences to ensure that, to the extent appropriate, information in the public domain is not subject to the secrecy offences (see subsections 122.5(2) and (8)).

114. In relation to whistleblowing, the secrecy regime ensures that a person can deal with information in order to make a disclosure to the Inspector-General of Intelligence and Security, the Commonwealth Ombudsman or the Law Enforcement Integrity Commissioner. The Bill also ensures that secrecy offences do not apply if a person communicates information in accordance with the *Public Interest Disclosure Act 2013*. These are well established processes for ensuring Commonwealth officers can report misconduct or corruption within the public sector, without publicly disclosing information. If a person makes the decision to disclose information that is inherently harmful or is likely to cause harm to Australia's interests outside of these processes, it is appropriate that they should be subject to the application of the secrecy offences.

115. The Bill contains protections for journalists, to ensure that the secrecy offences do not interfere with their ability to engage in fair and accurate reporting in the public interest, even if they have received information in breach of a secrecy offence (see subsection 122.5(6). The Bill does seek to criminalise the initial disclosure to a journalist of inherently harmful information or information that is likely to cause harm to Australia's interests but does not prevent a journalist who has received such information from using it in the public interest in the person's capacity as a journalist engaged in fair and accurate reporting.

116. The defence for journalists is limited by the requirement that the person must deal with or hold information in the public interest (see paragraph 122.5(6)(a)). The Bill provides that dealing with or holding information will not be in the public interest if it would, or is likely to, harm or prejudice the health or safety of the public or a section of the public or would constitute an offence under:

- section 92 of the *Australian Security Intelligence Organisation Act 1979* (publication of identity of ASIO employee or ASIO affiliate)
- section 41 of the *Intelligence Services Act 2001* (publication of identity of staff), or
- section 22, 22A or 22B of the *Witness Protection Act 1994* (offences relating to Commonwealth, Territory, State participants or information about the National Witness Protection Program.

117. These offences have been specifically excluded from being in the public interest because of the significant risks to a person's health and safety if they are identified as being a staff member of an intelligence agency or an informant for police or intelligence services.

Sabotage

118. Sabotage is criminalised in section 24AB of the Crimes Act.[60] The offence in section 24AB applies where a person carries out an act of sabotage or has in his or her possession any article that is capable of use, and which he or she intends for use, in carrying out an act of sabotage. An act of sabotage is defined to mean the destruction, damage or impairment, with the intention of prejudicing the safety or defence of the Commonwealth, of any article:

- that is used, or intended to be used, by the Defence Force or a part of the Defence Force or is used, or intended to be used, in the Commonwealth or a Territory not forming part of the Commonwealth, by the armed forces of a country that is a proclaimed country for the purposes of section 24AA;
- that is used, or intended to be used, in or in connection with the manufacture, investigation or testing of weapons or apparatus of war;
- that is used, or intended to be used, for any purpose that relates directly to the defence of the Commonwealth; or
- that is in or forms part of a place that is a prohibited place within the meaning of section 80.

119. The maximum penalty for the offence provided for in section 24AB is 15 years imprisonment.

The need for reform

120. The sabotage offence at section 24AB was first introduced into the Crimes Act in 1960, and has not been substantially amended since that time. As a result, the offence has not evolved to reflect the modern threat environment.

121. The offence, which is limited to the protection of defence facilities, does not account for other forms of infrastructure, the damage of which may cause serious harm to the safety of Australians or to Australia's national security interests. For example, by limiting sabotage to acts done in relation to defence facilities, the offence does not cover the sabotage of civilian technology or critical infrastructure not directly related to defence such as cyber infrastructure or telecommunications networks. Nevertheless, conduct which seeks to damage such infrastructure or services, which are essential to everyday

[60] *Crimes Act 1914 (Cth)* s 24AB.

life in Australia, could have a range of serious implications for business, governments and the community. The existing sabotage offence also fails to account for privately owned infrastructure despite the fact that the consequences flowing from damage to these types of infrastructure could be as harmful to Australia as damage to infrastructure owned by the Commonwealth.

122. As with espionage offences, the offence of sabotage also requires the prosecution to prove that a person intended to prejudice the safety or defence of the Commonwealth. Limiting sabotage to conduct which intends to prejudice the safety or defence of the Commonwealth does not recognise the significant harm that may result from acts of sabotage in circumstances in which a person lacks the relevant intent but nevertheless engages in the conduct. Furthermore, the requirement of intention may be difficult to prove beyond a reasonable doubt, particularly without disclosing sensitive information or capabilities.

123. Additionally, the existing sabotage offence does not prohibit preparatory conduct, such as introducing technical vulnerabilities in a product that will enable an act of sabotage at a later point. Although prohibiting the possession of an article capable of use in carrying out an act of sabotage partly covers preparatory conduct, the accompanying requirement that that article be intended for use in an act of sabotage does not provide for situations in a which a person is reckless as to this or for other preparatory conduct such planning for a sabotage offence.

124. Finally, the maximum penalty of 10 years imprisonment for a sabotage offence is relatively low when compared with the harm that could be caused by the commission of the offence, particularly in comparison to the penalties for espionage offences. In particular, there is no serious offence where a person intends or is reckless as to whether significant harm to national security will arise from the unauthorised activity.

125. To effectively protect Australia's interests, it is appropriate to ensure that sabotage offences cover the full range of infrastructure, the damage of which may cause significant harm to Australia's national security and the safety of Australian people. It is also necessary to ensure that the offences apply to conduct which may enable or result in the commission of a sabotage offence to allow law enforcement agencies to intervene before the damage occurs.

Outline of new sabotage offences

126. The Bill introduces a comprehensive range of sabotage offences into Division 82 of the Criminal Code, including:

- sabotage involving foreign principal (intention as to national security) - conduct *on behalf on 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 (penalty: 25 years imprisonment) [61]

- sabotage involving foreign principal (reckless as to national security) – conduct *on behalf of a foreign principal*, that results in *damage to public infrastructure*, *reckless* as whether the conduct will *prejudice Australia's national security* or advantage the national security of a foreign country (penalty: 20 years imprisonment)[62]

- sabotage (intention as to national security) – 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 (penalty: 20 years imprisonment)[63]

- sabotage (reckless as to national security) – conduct that results in *damage to public infrastructure*, *reckless* as whether the conduct will *prejudice Australia's national security* or advantage the national security of a foreign country (penalty: 15 years imprisonment)[64]

- introducing vulnerability (intention as to national security) – conduct that results in *public infrastructure* becoming *vulnerable to misuse, impairment or modification* with an *intention* to *prejudice Australia's national security or economic interests*; *disrupt* the functions of an Australian government or *damage* public infrastructure (penalty: 15 years imprisonment)[65]

- introducing vulnerability (reckless as to national security) – conduct that results in *public infrastructure* becoming *vulnerable to misuse, impairment or modification reckless* as to whether the conduct will *prejudice Australia's national security or economic interests*; *disrupt* the functions of an Australian government or *damage* public infrastructure (penalty: 10 years imprisonment)[66]

- preparing for a sabotage offence – conduct in *preparation* for, or *planning*, a *sabotage or introducing vulnerability offence* (penalty: seven years imprisonment).[67]

127. New sabotage offences will apply tiered penalties ranging from seven to 25 years imprisonment. This approach will ensure that the penalty for each offence is commensurate with the seriousness and culpability of offending. The lower penalties of seven years imprisonment will apply to sabotage-related offences such as preparing or planning for a sabotage offence. The highest penalty of 25 years imprisonment will apply

[61] Section 82.3
[62] Section 82.4
[63] Section 82.5
[64] Section 82.6
[65] Section 82.7
[66] Section 82.8
[67] Section 82.9

to the most egregious conduct, which involves conduct on behalf of a foreign principal which is intended to prejudice Australia's national security or advantage the national security of a foreign country. This penalty is significantly higher than the penalty of 10 years imprisonment for the existing sabotage offence.

128. The purpose of increasing the penalties for new sabotage 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, such as acts of sabotage on behalf of a foreign principal. It is necessary to apply a higher penalty for sabotage offences involving foreign principals because the involvement of a foreign principal in such an offence would undermine Australia's sovereignty and seriously threaten 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 to impose a heavier penalty where the consequences of the offence are particularly dangerous or damaging. Increasing penalties of imprisonment will also deter the commission of a sabotage offence.

129. For information on the penalty for each sabotage offence see **Appendix D**.

Key changes to sabotage offences

130. The key changes to sabotage offences include:

- the protection of a broader range of infrastructure
- the criminalisation of a broader range of conduct which causes damage
- the introduction of offences involving a foreign principal
- the introduction of offences of recklessness
- the introduction of offences undertaken on behalf of a foreign principal
- the introduction of 'introducing vulnerability' offences
- the introduction of an offence to prepare or plan for a sabotage offence
- the introduction of a specific defence to an offence of sabotage.

Public infrastructure

131. New sabotage offences will criminalise conduct causing damage to a broad range of public infrastructure, including:

- 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 1903*
- service property and service land, within the meaning of the *Defence Force Discipline Act 1982*
- 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 the public with utilities or services is located in Australia, and belongs to or is operated by a constitutional corporation or is used to facilitate constitutional trade and commerce.[68]

132. By broadening the range of infrastructure beyond defence facilities, the new sabotage offences will cover the damage of infrastructure and services that are essential to everyday life in Australia. The definition has been developed to cover such infrastructure to the extent possible, consistent with the Australian Government's power to legislate under the Constitution.

Damage to public infrastructure

133. The new sabotage offences will also broaden the types of conduct which cause damage to public infrastructure, including conduct which:

- destroys or results in destruction of infrastructure
- involves interfering with, or abandoning infrastructure, resulting in it being lost or rendered unserviceable
- results in infrastructure suffering a loss of function or becoming unsafe or unfit for its purpose
- limits or prevents access to infrastructure by persons who are ordinarily entitled to access it or that part of it
- results in infrastructure becoming defective or being contaminated
- significantly degrades the quality of infrastructure, or
- if it is an electronic system—seriously disrupts infrastructure.[69]

134. By broadening the meaning of 'damage to public infrastructure', the new offences will capture the full range of conduct and methodologies currently undertaken by foreign

[68] Section 82.2
[69] Section 82.1

adversaries and other persons who seek to harm Australia's interests. The expanding of conduct which causes damage is also necessary to reflect the broader range of infrastructure now covered by the offences.

Sabotage involving a foreign principal

135. The Bill will introduce specific sabotage offences which apply where a person engages in conduct on behalf of, or directed, funded or supervised by, a foreign principal or a person acting on behalf of a foreign principal. The introduction of these offences recognises the serious consequences that may result from acts of sabotage undertaken on behalf of a foreign principal, which seriously undermines Australia's sovereignty and national security.

136. The offences will apply tiered penalties ranging from 20 to 25 years imprisonment and will depend upon the seriousness of the offence and the culpability of the offender. Where an offence on behalf of a foreign principal is committed with an intention to prejudice Australia's national security or advantage the national security of a foreign country, a maximum penalty of 25 years imprisonment applies. This penalty is appropriate to deter and punish a worst case offence which may result in Australians being 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. The risks that may be posed to the safety and security of Australians and Australia's interest's by such damage are very high and it is appropriate that the offence be punishable by a serious penalty.

Recklessness offences

137. New sabotage offences will implement a tiered approach, covering both intentional and reckless conduct. The introduction of offences for recklessness addresses the significant harm that may result from acts of sabotage in circumstances in which a person lacks the relevant intent but nevertheless engages in the conduct. The recklessness offences are designed to capture the full range of conduct undertaken by foreign actors and other persons seeking to damage Australia's public infrastructure.

138. Under section 5.4 of the Criminal Code, the fault element of recklessness provides that a person is reckless with respect to a circumstance or a result if he or she is aware of a substantial risk that the circumstances exists or will exist or the result will occur and having regard to the circumstances known to him or her, it is unjustifiable to take the risk. For a sabotage offence, a person will need to be aware of the substantial risk that their 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 the risk.

139. As with the espionage offences (discussed above at paragraphs 47-49), the benefit of adding sabotage offences that have recklessness as a fault element is ensuring that offences and penalties are appropriately tailored to the level of culpability of the offence. It allows for tiered penalties to be applied, recognising that the most serious

offences – where a person intended to prejudice Australia's national security or advantage the national security of a foreign country – should attract a more significant penalty commensurate with the person's culpability, while lower penalties apply where recklessness is the fault element. Furthermore, a tiered approach provides a range of options to law enforcement and prosecutorial agencies when investigating sabotage offences.

Introducing vulnerability offences

140. New Division 82 introduces offences for 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, with an intention 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.[70]

141. The offence will be punishable by a penalty of 10 to 15 years imprisonment, depending upon whether the person engaging in the conduct intents to or is reckless as to whether their conduct harms Australia national security. 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.

Preparing or planning for a sabotage offence

142. The Bill will introduce an offence to prepare for or plan an offence of sabotage or introducing vulnerability.[71] 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 an offence is committed or public infrastructure is damaged.

143. 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, this offence is intended to capture behaviour at the planning stage, rather than the more advanced stage at which an ancillary offence of attempt would otherwise apply.

Treason, treachery and other threats to security

144. The Bill will amend Part 5.1 of the Criminal Code to modernise and simplify Australia's treason and treachery offences and to ensure that the offences appropriately reflect modern terminology related to armed conflict.

[70] Sections 82.7 - 82.8
[71] Sections 82.9

145. The Bill will also introduce new Division 83 into the Criminal Code. Division 83 will modernise and improve the existing offences against the government in Part II of the Crimes Act, which will be repealed. The offences in Division 83 will protect Australia's defence by criminalising conduct which advocates mutiny, assists prisoners of war to escape and involves military-style training by foreign governments. New Division 83 will continue to criminalise interference with Australian democratic or political rights where the conduct involves the use of force, violence or intimidation.

Treason

146. Treason is criminalised in Division 80 of the Criminal Code. Division 80 contains a number of treason offences including the offences of 'Assisting enemies at war with the Commonwealth' (subsection 80.1AA(1)) and 'Assisting countries etc. engaged in armed hostilities against the ADF' (subsection 80.1AA(4)).

147. The offence at subsection 80.1AA(1) applies if the Commonwealth is at war with an enemy and a person engages in conduct with an intention to materially assist the enemy to engage in war with the Commonwealth, and the conduct assists the enemy to engage in the war. The offence provided for at subsection 80.1AA(4) applies if a country or organisation is engaged in armed hostilities against the Australian Defence Force (ADF) and a person engages in conduct with an intention to materially assist the country or organisation that is engaged in armed hostility against the ADF and the conduct assists the country or organisation to engage in the armed hostilities.

148. For the offences at section 80.1AA to apply, the person engaging in the relevant conduct must be an Australian citizen or resident, be voluntarily under the protection of the Commonwealth of Australia, or be a body corporate incorporated by or under a law of the Commonwealth, State or Territory. The offences are punishable by a maximum penalty of life imprisonment.

149. The treason offences provided for in section 80.1AA of the Criminal Code no longer reflect international terminology relating to armed conflict. Under international law, the term 'war' is no longer used nor does the practice of 'declaring war' occur in modern conflict. Similarly, the reference to 'armed hostilities' in subsection 80.1AA(4) does not accurately reflect the current international lexis. The phrase 'engaging in armed conflict' is the preferred terminology, which is consistent with various other provisions of the Criminal Code including offences against the United Nations in Division 71 and war crimes offences in Division 268.

150. Furthermore, as noted by the Gibbs Review of Criminal Law[72], the distinction between being a person 'against whom the Defence Force is opposed' and being an 'enemy at war with the Commonwealth' is not 'so great or so useful as to justify separate offences' as is currently the case in section 80.1AA.

[72] Review of Commonwealth Criminal Law – Final Report, Sir Harry Gibbs, December 1991.

151. To address these issues, the Bill will repeal existing section 80.1AA of the Criminal Code and combine the offences at subsections 80.1AA(1) and 80.1AA(4) into a single new offence of 'Treason – assisting enemy to engage in armed conflict'. The new offence will apply where a person engages in conduct with an intention to materially assist an enemy engaged in armed conflict involving the Commonwealth or the Australian Defence Force where the conduct materially assists the enemy to engage in the armed conflict. Consistent with the existing treason offences, the new offence will carry a maximum penalty of life imprisonment and will only apply to persons who knowingly owe an allegiance to the Commonwealth.

152. The new offence will simplify the structure of the existing treason offences, update the references in the offences to reflect modern international terminology relating to armed conflict and remove the confusing language at existing subsection 80.1AA(4) regarding 'armed hostilities'.

153. Although rarely used, treason offences are a critical part of Commonwealth criminal law. Treason offences seek to ensure the protection of Australia against the actions of its own citizens who seek to undermine the operational security or effectiveness of the defence force by providing assistance to an enemy in engaged in armed conflict against Australia. At its core, treason represents a violation or betrayal of a person's allegiance to Australia. Given the seriousness of treason offences and the significant penalties that apply, it is appropriate that the law achieves the highest degree of certainty, by removing ambiguity and ensuring consistency with related offences across the Commonwealth statute book.

Treachery

154. Treachery is criminalised in section 24AA of the Crimes Act. The offence in section 24AA applies where a person engages in conduct with an intention to overthrow the constitution of the Commonwealth by revolution or sabotage or to overthrow by force or violence the established government of the Commonwealth, a State or a proclaimed country. Section 24AA also applies to conduct levying war against a proclaimed country, instigating a person to make an armed invasion of a proclaimed country or assisting any person against whom the Australia Defence Force is opposed.

155. Under section 24AA, a proclaimed country means a country specified by proclamation and includes any colony, overseas territory or protectorate of that country, or any territory for the international relations of which that country is responsible, which is a colony, overseas territory, protectorate or territory to which the proclamation is expressed to extend.

156. The treachery offences provided for in section 24AA are duplicative of existing offences in the Commonwealth criminal law including the treason offences of assisting enemies at war with the Commonwealth and countries engaged in armed hostilities against the ADF at subsection 80.1AA, as well as foreign incursion offences provided for in Part 5.5 of the Criminal Code, which deal with hostile activities intended to overthrow the government of a foreign country.

157. The Bill will create a new offence of treachery in Division 80 of the Criminal Code which 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 existing treachery offence at subsection 24AA(1), which relates to acts intended to overthrow the government of a proclaimed country, will not be replicated in the new offence as such acts are currently criminalise by foreign incursion offences. Similarly, the existing treachery offence at subsection 24AA(2), which relates to assisting enemies of the ADF, will not be replicated in the new treachery offence as such conduct will be covered by the new treason offence.

158. The introduction of the new offence will eliminate duplication and simplify the structure the existing offence. By transferring the new offence to Division 80 of the Criminal Code the offence will appropriately complement treason offences as well the offence of urging violence against the Constitution which is provided for at section 80.2 of the Criminal Code.

Other threats to security

Advocating mutiny

159. The existing offence of 'inciting mutiny' in section 25 of the Crimes Act criminalises intentional conduct attempting to incite any person serving in the Queen's Forces to commit an act of mutiny or to make a mutinous assembly or to seduce any person serving in the Queen's Force from his or her duty or allegiance. Under section 25, a person serving in the Queen's Forces includes any person serving in an arm of the defence force of Australia, the United Kingdom or a British Possession. The maximum penalty for this offence is life imprisonment.

160. The offence at section 25 was enacted in the original Crimes Act in 1914 and has not been substantively amended since that time. As a result, the offence has not evolved to reflect the modern Australian context. References to the 'Queen's Forces' for example, inappropriately extends the offence to inciting members of the United Kingdom defence force, as well as those forces of a British dominion, to commit an act of mutiny. This is inconsistent with the offence of mutiny provided for in section 20 of the *Defence Force Discipline Act 1982* (the Defence Force Discipline Act), which is limited to acts of mutiny undertaken by persons who are members of the Australian Defence Force.

161. The penalty of life imprisonment for the current offence also fails to reflect contemporary standards of seriousness. It is not appropriate or consistent with the principles for establishing criminal penalties for an offence of inciting 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 at subsection 20(2) of the Defence Force Discipline Act, particularly where the less serious mutiny offence at subsection 20(1) only carries a penalty of 10 years imprisonment.

162. In addition, the existing offence has not been amended to take into the codification of attempt and incitement as extensions of criminal responsibility in Chapter 2 of the

Criminal Code.[73] For example, the existing offence requires proof that a person 'intentionally attempts' to 'incite' a person to commit an act of mutiny. This combination of extensions of criminal responsibility creates confusion about what would be required to be proved in order to establish the offence, taking into account the provisions in Chapter 2 of the Criminal Code about attempt and incitement.

163. To modernise and improve the offence of inciting mutiny at section 25 of the Crimes Act, the Bill will replace the existing offence with the new offence of 'advocating mutiny' at section 83.1 of the Criminal Code. The new offence, punishable by a maximum penalty of seven years imprisonment, will apply where a person advocates mutiny, reckless as to whether the result will be that a defence member takes part in a mutiny.

164. The new offence will broaden the type of conduct which may result in a member of the defence force taking part in a mutiny by replacing the term 'inciting' with the term 'advocating'. The term 'advocating' is intended to take its ordinary meaning and could include supporting, recommending, promoting, encouraging or urging in addition to inciting. By using the word 'advocating' instead of 'inciting' the offence will further eliminate duplication with respect to the extension of criminal responsibility under section 11.4 ('incitement') of the Criminal Code. Similarly, by removing the confusing element of 'attempt' the new offence will also eliminate duplication with respect to section 11.1 ('attempt') of the Criminal Code.

165. To ensure consistency with equivalent Commonwealth criminal offences, the new offence is based on the offences of advocating terrorism in section 80.2C and advocating genocide in section 80.2D of the Criminal Code. The new offence will also replace references to the 'Queen's Force' with the 'Australian Defence Force' and lower the penalty of imprisonment in order for the offence to complement the offence at section 20 of the *Defence Force Discipline Act 1982.*

Assisting prisoner of war to escape

166. Assisting prisoners of war to escape is criminalised in section 26 of the Crimes Act. This offence applies where a person intentionally aids an alien enemy who is a prisoner of war to escape, or in their escape, from a prison or place of confinement, or from the Commonwealth or a Territory not forming part of the Commonwealth. The offence is punishable by life imprisonment.

167. The Department of Defence has advised that this offence is still required because it is foreseeable that the Australian Defence Force could be involved in detention operations if Australia was engaged in an international armed conflict. As civilians are increasingly a part of military operations and deployments, as contractors or non-military Defence personnel, a general offence remains necessary.

[73] Sections 11.1 to 11.6 of the Criminal Code

168. The Bill will replicate the existing offence of assisting prisoners of war to escape at section 26 of the Crimes Act (which will be repealed) in new Division 83 of the Criminal Code. The new offence will apply 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.

169. The key change between the offences is that the new offence will significantly reduce the maximum penalty from life imprisonment to 15 years imprisonment. The current offence for assisting prisoners of war to escape was enacted in the original Crimes Act in 1914. The penalty of life imprisonment no longer reflects contemporary standards of seriousness for the offence. The new maximum penalty of 15 years imprisonment is comparable with maximum penalties for other offences relating to escaping criminal detention, including section 47A of the Crimes Act which carries a penalty of 14 years imprisonment for the offence of rescuing a prisoner from criminal detention.

Interference with political rights and duties

170. Section 28 of the Crimes Act criminalises conduct which uses violence, threats or intimidation to hinder or interfere with the free exercise of another person's political rights or duties. This offence is punishable by three years imprisonment.

171. The Bill will replicate the existing offence of interfering with political liberty at section 28 of the Crimes Act (which will be repealed) in new Division 83 of the Criminal Code. The new offence will apply where a person uses force, violence, threats or intimidation to interfere with another person's Australian democratic or political right under the Constitution or Commonwealth law.

172. The limitation to 'Australian' democratic and political rights is intended to limit the operation of the offence 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.

173. By requiring the rights affected to be rights arising under the Constitution or a law of the Commonwealth the offence is further limited to the Commonwealth jurisdiction. This ensures that interference with democratic and political rights which arise under a state and territory law are not captured. This is appropriate as individual rights and duties vary considerably between states and territories. The limitation of the offence to political rights and duties arising under the Constitution or a Commonwealth law also implements the recommendation of the Gibbs Review of Criminal Law to amend the offence in order to remove any doubt as to its application to the rights and duties of a Member of Parliament.

174. The new offence will be punishable by a maximum penalty of ten years imprisonment. This penalty is considerably higher than the maximum penalty of three years for the existing offence. The increase in penalty reflects the current threat

environment in which an increasing number of foreign actors seek to interfere in and/or influence Australia's political processes and the exercise of Australian democratic or political rights. The new penalty aims to deter the commission of the offence.

Military-style training involving foreign government principal

175. Subsection 27(1) of the Crimes Act makes it an offence for a person to train or drill any other person to the use of arms or the practice of military exercises, movements or evolution in contravention of the directions of a proclamation by the Governor-General. Section 27(1) also applies to conduct of a person who is present at any meeting or assembly of persons for the purpose of training or drilling any other person to the use of arms or the practice of military exercises, movements, or evolutions. The offences are punishable by five years imprisonment. Subsection 27(2) further makes it an offence for any person who, at any meeting or assembly held in contravention of the directions of a proclamation by the Governor-General, is trained or drilled to the use of arms or the practice of military exercises, movements, or evolutions. This offence is punishable by a maximum penalty of two years imprisonment.

176. Under the offences of unlawful drilling at section 27 of the Crimes Act, no proclamation of the Governor-General has ever been made, despite the existence of the offences since the first enactment of the Crimes Act. Furthermore, the undertaking of military training for armed warfare may also be captured by terrorism offences provided for in Part 5.3 of the Criminal Code as well the new treachery offence relating to the use of force or violence to overthrow the Constitution or an Australian government.

177. As such, the Bill will repeal the existing offence of unlawful drilling and introduce a new offence of 'military-style training involving foreign government principal'. The new offence will apply where a person provides, receives or participates in training that involves using arms or practising military exercises, movements or evolutions, when that training is provided on behalf of a foreign government principal, or is directed, funded or supervised by a foreign government. Appropriate defences will 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.

178. The new offence is punishable by a maximum penalty of 20 years imprisonment. This penalty 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.

False or misleading information

179. Schedule 3 will amend Division 137 of the Criminal Code to introduce a new aggravated offence for providing false or misleading information.

180. Under the underlying offence (punishable by 12 months imprisonment), a person provides false or misleading information by providing information which is false or misleading or omits any matter or thing without which the information is misleading to a Commonwealth entity, a person exercising powers or functions under or in connection with a law of the Commonwealth or in compliance with a law of the Commonwealth.[74]

181. The new aggravated offence will apply where a person provides false or misleading information in relation to an application for, or maintenance of, an Australian Government security clearance.[75] The aggravated offence will be subject to the defences provided for by the underlying offence which apply where the information is not false or misleading, or where the Commonwealth does not take reasonable steps to inform the person providing the information of the existence of the offence, before the information is provided.[76] The aggravated offence will be punishable by a maximum penalty of five years imprisonment.

182. The introduction of the aggravated offence is necessary to address 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. For example, 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.

183. In this respect, the aggravated offence will strengthen and support a number of other offences provided for in the Bill, namely espionage, theft of trade secrets and secrecy, by reducing the risk posed by those who seek to access or disclose classified information for the purpose of harming Australia's interests or advantaging the interests of a foreign country. The aggravated offence will also support sabotage offences by deterring conduct involving access to public infrastructure or classified information relating to public infrastructure by persons who seek to damage or otherwise leave infrastructure vulnerable to misuse, impairment or modification.

184. The introduction of the aggravated offence which carries a substantially higher penalty is also 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.

TIA Act amendments

185. Schedule 4 amends the definition of a 'serious offence' in subsection 5D(1)(e) of Part 1.2 of the TIA Act to include the new offences provided for in:

[74] Subsection 137.1(1)
[75] Subsection 137.1A(1)
[76] Subsection 137.1A(3)

- 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).

186. A 'serious offence' for the purpose of the TIA Act is one for which declared agencies can seek interception warrants.

187. 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

188. Equivalent amendments are not required to allow other law enforcement powers, such as surveillance devices, controlled operations or assumed identities. These regimes already apply to the offences created by the Bill. For example, section 14 of the *Surveillance Devices Act 2007* (Cth) allows a surveillance device warrant to be issued in relation to relevant offences. This term is defined in section 6 to mean a Commonwealth offence with a maximum term of imprisonment of 3 years or more or for life.

Legislative safeguards

189. Many of the legislative safeguards which apply to the offences have been set out in the Explanatory Memorandum to the Bill, particularly the Statement of Compatibility with Human Rights. These safeguards include, for example, the availability of offence-specific defences, and the application of 'consent to prosecute' provisions.

190. Offence-specific defences will be available for the offences of sabotage, espionage, foreign interference and secrecy. These defences will primarily apply to conduct in a person's capacity as a public official or in accordance with a law or agreement of the Commonwealth. For secrecy offences, specific defences will also apply where the information communicated or otherwise dealt with is already publicly available; is held for the purposes of fair and accurate reporting; or is communicated to the Inspector-General of Intelligence and Security, the Commonwealth Ombudsman or the Law Enforcement Integrity Commissioner, to a court or tribunal or in accordance with the *Public Interest Discourse Act 2013*.

191. In addition to specific defences, the general defences under Part 2.3 of the Criminal Code will be available for all offences.[77] 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.

192. The application of defences will allow a person accused of an offence provided for in the Bill to justify their actions and defend the criminal charge against them.

193. A further safeguard provided for by the Bill is the requirement of the Attorney-General's consent prior to the prosecution of an offence of espionage, theft of trade secrets, foreign interference, sabotage or other threats against security.[78]

194. 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. This individualised assessment prior to prosecution is intended to ensure that proceedings are only commenced where the Attorney-General has assessed that it is appropriate to do so in all the circumstances.

195. The Bill also considers the appropriate application of the extensions of criminal responsibility in Chapter 2 of the Criminal Code, by disapplying the application of section 11.1 of the Criminal Code (attempt) for the preparatory offences. Given that these offences already target preparatory conduct, the application of attempt would inappropriately extend criminal responsibility to conduct that was at such an early stage that it did not warrant criminal sanction.

196. The Bill will also provide specific safeguards for journalists in respect of secrecy offences, which is discussed in further detail at paragraphs 114 and 115 of this submission.

197. For a more detailed analysis of the balance between the protection of national security and individual rights and freedoms see the Statement of Compatibility with Human Rights at page 6 of Explanatory Memorandum to the Bill.

[77] These defences are in sections 7.1 to 10.5 of the Criminal Code
[78] Sections 82.13, 83.5 and 93.1

Appendix A – ASIO unclassified conduct examples

Activity: Espionage (conspiracy)

Person 1 was an Australian citizen who agreed to undertake specific tasking from a foreign individual whom Person 1 knew to be a foreign intelligence service (FIS) officer. At the request of the FIS officer, Person 1 used their professional duties to obtain security classified Australian Government information and other privileged information concerning national security, and passed such material to the FIS officer in return for payment. Person 1 was aware the FIS officer made arrangements to conceal this relationship from Australian authorities by employing covert communication and meeting techniques.

Activity: Espionage (soliciting/conspiracy); Foreign Interference

Person 2 was an Australian national who worked as a conscious facilitator for a foreign intelligence service (FIS), assisting the FIS to undertake intelligence activity in Australia. Using their Australian nationality and employment to develop access, Person 2 cultivated and recruited an Australian official to provide privileged information concerning Australia's national security to the FIS. Person 2 undertook these activities in conscious collaboration with a FIS officer in order to advance the national security of the foreign country, and facilitated payments from the FIS officer to the Australian official in return for this privileged information. Person 2 also pursued information for intelligence purposes regarding other Australian officials who might be useful to the FIS and were potentially vulnerable to intelligence targeting, for referral to the FIS officer.

Activity: Foreign interference (support to a foreign intelligence agency)

Person 3 was a naturalised Australian national who was sent to Australia by a foreign intelligence service (FIS) to serve as a 'sleeper' agent. Person 3 built community and business links while establishing a life in Australia over decades, and consciously maintained direct and electronic contact with FIS officers. Person 3 provided extensive information to the FIS about Australia-based expatriate dissidents, which was used to support FIS harassment of these dissidents and their relatives overseas. Person 3 also provided logistical support to FIS officers travelling to Australia to conduct intelligence activity. Person 3 was rewarded for these activities with significant cash payments.

Activity: Espionage (preparatory offences/conspiracy); Secrecy (unauthorised removal of security classified information)

Person 4 was an Australian citizen who was employed in the Australian Government. During their employment and without authorisation, Person 4 removed a large volume of electronic media from its proper place of custody at their workplace, and inappropriately stored large amounts of materials, including security classified material, at t heir residence. When approached by a self-identified foreign intelligence service (FIS) officer, Person 4 agreed to assist the FIS officer to obtain Australian security classified information and advantage that foreign country, and divulged details about Australian Government computer networks, operations and vulnerabilities to the FIS officer.

Activity: Secrecy (unauthorised disclosure of privileged information; unauthorised removal of security classified information)

Person 5 was an Australian citizen, who was employed in the Australian Government. During their employment and without authorisation, Person 5 removed security classification information from its proper place of custody at their workplace and posted it online, divulging Australian Government and partner information to the public. The public exposure of this security classified information was harmful to Australia's national security for the potential to damage Australian and partner capabilities and relationships, and the information was likely to have been of high interest and value to hostile foreign intelligence services.

Activity: Foreign Interference (preparatory conduct); False and misleading statements (related to security clearance)

Person 6 was an Australian citizen who undertook training activities overseas, provided by a foreign intelligence service (FIS). When Person 6 later applied for a security clearance with the Australian Government, they did not declare the FIS training in information provided to vetting authorities, including in response to direct questions about foreign government associations. These false statements meant Person 6 was granted a security clearance and access to information that would not have otherwise been authorised, presenting significant potential harm to Australian and allied interests.

Appendix B – Comparison of international regimes

Espionage

United States

US espionage offences are found in 18 USC Chapter 37 (Espionage and censorship). The provisions deal with documents, material or information related to the national defence. Key offences are:

- Communicating certain classified information to an unauthorised person or publishing certain classified information in any manner prejudicial to the safety or interest of the US or for the benefit of any foreign government to the detriment of the US (18 USC § 798)
- Gathering, transmitting to an unauthorised person, or losing information pertaining to the national defence, and conspiracies to commit such an offence (18 USC § 793)
- Delivering or attempting to deliver to agents or subjects of foreign countries information pertaining to the national defence of the US, with intent or reason to believe that it will be used to injure the US or be used to the advantage to the foreign nation (18 USC § 794)
- Wartime espionage (18 USC § 798A).

The US also has specific provisions directed at economic espionage (18 USC § 1831) and computer espionage which, anecdotally at least, are used to prosecute cases where the threshold for espionage cannot be met.

The US has successfully prosecuted espionage offences in recent times. These include a former army lieutenant who pleaded guilty to passing classified national defence information to his Chinese girlfriend, and an FBI agent who was a double agent working for Beijing. Other cases include the case of a naturalised American allegedly running a spy ring aimed at stealing nuclear secrets, and a US naval officer who is accused of passing on US naval secrets to a foreign country.

Canada

Section 16 of the *Security of Information Act 1985* (SOI Act) sets out the offence of communicating safeguarded information, which occurs when:

- a person communicates to a foreign entity[79] or terrorist group[80] information that the Government of Canada has taken measures to safeguard[81]
- the person either believes, or is reckless as to whether the information is information that is 'safeguarded', and
- in communicating the information, the person intends to increase the capacity of that entity or group, or is reckless about whether the communication of the information is likely to increase capacity; or that harm to Canada or Canadian interest results from the unlawful communication.

The offence carries a maximum penalty of life imprisonment.

Section 17 of the SOI Act sets out the offence of communicating special operational information. This offence is framed in similar terms to that in section 16, including that the person must intentionally communicate the information to a foreign entity or terrorist group, and believe or be reckless as to whether the information is special operational information. However, there is no need to prove that either actual harm resulted or that there was an intent to increase the capacity of the foreign entity or group (communication alone attracts the criminal liability). This offence also carries a sentence of life imprisonment.

Finally, section 18 of the SOI Act sets out the offence of 'breach of trust in respect of safeguarded information.' This offence applies to persons with a security clearance granted by the Government of Canada, where that person intentionally and without lawful authority, communicates (or agrees to communicate) to a foreign entity or terrorist group any information the Government of Canada is taking measures to safeguard. This offence attracts a maximum penalty of two years' imprisonment. Similar to the offence at section 17, the prosecution need not prove that actual harm occurred because of the disclosure, or that the person intended to increase the capacity of the foreign entity or terrorist group.

---

[79] 'Foreign entity' is defined in subsection 2(1) of the SOI Act as 'a foreign power; a group or association of foreign powers, or one or more foreign powers and one or more terrorist groups; a person acting at the direction or, for the benefit of, or in association with a foreign power.

[80] 'Terrorist group' is defined in the SOI Act as having the same meaning as in subsection 83.01(1) of the *Criminal Code*, which provides (a) an entity that has as one of its purposes or activities facilitating or carrying out any terrorist activity, or (b) a listed entity, and includes an association of such entities.

[81] 'Safeguarded information is not defined in the Act, however 'Special operational information" is defined in section 8 of the SOI Act. It is 'information that the Government of Canada is taking measures to safeguard that reveals, or from which may be inferred: the identity of a person, agency, group, body or entity which is, or is intended to be, a confidential source of information, intelligence or assistance to the Government; nature or content of plans for military operations in respect of armed conflict; means used, intended to be used, or capable of being used to covertly collect, obtain, decipher, assess, analyse, communicate or otherwise deal with information or intelligence; whether a place, person, agency, group, body or entity was/will be the object of a covert investigation; means used, or capable of being used, by the Government to protect or exploit the above information/intelligence; information or intelligence similar in nature to the information referred to above, that is in relation to, or received from, a foreign entity or terrorist group.

In addition to these offences, section 19 of the SOI Act also has offences that specifically cover economic espionage and the use/theft of trade secrets for the benefit of a foreign entity. However, while these laws exist, there have been no successful prosecutions. Economic espionage offences are discussed in greater detail in a separate paper.

New Zealand

Espionage is covered by section 78 of the *Crimes Act 1961*. The provisions cover the act of communicating information to any country or organisation, or to an agent of any country or organisation with the intent to prejudice the security or defence of New Zealand.[82] There is also an offence for acts preparatory to communicating information to any country or organisation, including collecting or recording information, copying or obtaining a document, or making a sketch, recording or note. The offences carry a maximum penalty of 14 years' imprisonment.

Section 78A provides that it is an offence for people who hold government security clearances, or those with access to classified information to wrongfully communicate, retain or copy it. The maximum penalty is three years imprisonment.

United Kingdom

The *Official Secrets Act 1911-1989 (UK)* provides the principal legal protection in the UK against espionage and unauthorised disclosure.

The espionage provisions cover situations where a person obtains or communicates to any other person information relating to security or intelligence. The provisions in the *Official Secrets Act 1989* create an offence for the unlawful disclosure of information in six specific categories[83] by employees and former employees of security and intelligence services[84] and for current and former Crown servants and Government contractors. The maximum term of imprisonment for offences relating to espionage is fourteen years.

Theft of trade secrets

United States

The *Economic Espionage Act 1996* (EEA) within the US Criminal Code (USC) was enacted in 1996 in response to several Committee recommendations to the US

[82] The country or organisation in question is irrelevant; it is the intended effect of 'prejudicing the security or defence of New Zealand' which matters.
[83] The six categories are 'security and intelligence, defence, international relations, information obtained in confidence from other states or international organisations, information likely to result in the commission of an offence, or likely to impede detection, and special investigations under statutory warrant (e.g. interception of communications).'
[84] Intelligence and security service employees face an 'absolute' test, rather than a 'damage' test as applies to other employees/contractors. Team considering whether we should reflect an absolute test as an option here (noting we will likely cover during broader secrecy offence analysis).

Congress. The relevant provisions in the Act are cast broadly and have two effects: to make theft of trade secrets a crime; and to make economic espionage a crime.

In the US, it is a federal criminal offence for any person to unlawfully acquire covert trade secrets for their own benefit or the benefit of others, intending or knowing that the offence will injure any owner of the trade secret. The EEA protects against theft that occurs either in the US, or outside the US, where the responsible individual is either a citizen or permanent resident, or the responsible entity is organised under US laws.

The EEA defines a trade secret as all forms of information,[85] however stored and maintained, if reasonable efforts have been made to keep the information secret and if the information has independent economic value.[86]

18 USC 1831 prohibits economic espionage, which involves a person or organisation knowingly stealing, duplicating or possessing trade secrets or engaging in preparatory or conspiring acts, where there is intent or knowledge for the offence to benefit any foreign government, foreign instrumentality or a foreign agent. This offence carries a maximum imprisonment of 15 years and/or maximum fine of $5 million for an individual and a maximum fine of the greater of $10 million or three times the value of the trade secret for any corporation or organisation.[87]

In contrast to the economic espionage provisions of 18 USC 1832, which requires a foreign beneficiary, 18 USC 1831 is a general criminal 'theft of trade secrets' offence. 18 USC 1831 prohibits a person or organisation knowingly stealing, duplicating or possessing trade secrets or engaging in preparatory or conspiring acts to steal, duplicate or possess trade secrets. For the offence to apply, there must be intent to convert a trade secret, that is related to products or services used or intended for use in interstate or foreign commerce, to an economic benefit for anyone other than the owner of the trade secret. There must also be intent or knowledge that the offence will injure the owner of the trade secret. This offence carries a maximum imprisonment of 10 years and/or maximum fine of $500,000 for an individual and a maximum fine of the greater of $5 million or three times the value of the trade secret for any corporation or organisation.[88]

There is also criminal forfeiture to the US of any property constituting or derived from the proceeds of violations of the EEA, and the forfeiture of any property used or intended to be used, in any manner or part, to commit or facilitate a violation of the EEA.[89]

---

[85] This includes information that is financial, business, scientific, technical, economic or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes whether tangible or intangible.
[86] Therefore, a trade secret is different from a patent or copyright whereby owners may sue under patent or copyright laws.
[87] This includes expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided.
[88] Same provision as footnote 7 applies.
[89] 18 USC 1834.

The Attorney-General has civil relief in civil proceedings to issue orders to seize property and grant injunctions to preserve confidentiality of trade secrets. There is a three year limitation on bringing civil action.[90]

The EEA does not prohibit or create a private right for:[91]

- any otherwise lawful activity conducted by the US government;
- disclosure of trade secrets that are made in confidence to a public official either directly or indirectly, or to an attorney for the sole purpose of reporting or investigation suspected violations of law;
- disclosure of trade secrets made in a document filed under seal in a law suit.

Between 1996 and 2012, there were nine indictments made under 18 USC 1831 and 115 indictments made under 18 USC 1832.[92] Between 1996 and 2016 there have been six convictions under 18 USC 1831:

- *United States v. Fei Ye & Ming Zhong* (2006) NDCA: Two defendants stole microchip blueprints from Silicon valley to benefit China and were sentenced to 1 year imprisonment;

- *United States v. Xiaodong Meng* (2006) NDCA: Defendant misappropriated a trade secret from a private company used for military training and other purposes for the benefit of China and was sentenced to two years imprisonment with three years of supervised release. They were also required to pay a fine of $10,000 and forefeit computer equipment seized in the case.

- *United States v. Dongfan 'Greg' Chung* (2011) CDCA: Former Boeing engineer sentenced to 188 months imprisonment and 3 years supervised release for giving aviation technology information to China.

- *United States v. Kexue Huang* (2011) CDIN: Pleaded guilty to exporting $300 million worth of trade secrets to China and Germany through an intermediary and was sentenced to 87 months in prison and 3 years of supervised release.

- *United States v. Elliot Doxer* (2011) D.Mass: Sentenced to 6 months in prison with 2 years of supervised release, and fined $25,000 for disclosing trade secrets over an 18-month period to an undercover federal agent posing as an Israeli intelligence officer.

- *United States v. Walter Liew, & USA Performance Technology, Inc.* (2014) NDCA: Sentenced to 15 years imprisonment and ordered to forfeit $27.8 million in illegal profits and pay a fine of $511,667.82 for engaging in economic espionage, tax evasion, bankruptcy fraud, and obstruction of justice.

On many occasions, whilst indictments were initially filed with an 18 USC 1831 charge, they would eventually be dropped in favour of defendant's pleading guilty to the lesser

[90] 18 USC 1836.
[91] 18 USC 1833.
[92] Law360 – Lexis Nexis, *A Look at 16 Years of EEA Prosecutions*. 2012, viewed August 2017, http://www.law360.com/articles/378560/a-look-at-16-years-of-eea-prosecutions (Lexis Nexis Article 2012).

charge of stealing trade secrets under 18 USC 1832.[93] The greater amount of indictments and convictions under theft of trade secret (18 USC 1832) over economic espionage (18 USC 1831) is predominately due to the fact that the theft of trade secret offence does not require proving a connection to a foreign beneficiary and therefore is easier to prosecute.

In 2015, six Chinese nationals, including three professors, who studied and worked in the US before returning to China with allegedly stolen wireless technology, were charged with economic espionage and theft of trade secrets as well as conspiracy to commit such offences and aiding and abetting.[94] The prosecutions have yet to be finalised.

Canada

Section 19 of the Canadian *Security of Information Act* (SOI Act) criminalises economic espionage. It prevents a person from communicating, obtaining, retaining, altering or destroying a trade secret destroyed fraudulently and without colour of right[95] at the direction of, for the benefit of or in association with a foreign economic entity and to the detriment of Canada's economic interests, international relations, national defence or national security. The offence is punishable by up to 10 years' imprisonment and 2 years imprisonment for preparatory acts.[96] A 'trade secret' is defined as any information (including a negotiation position or strategy, or any information embodied in a 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.

A defence to economic espionage applies if the trade secret was obtained through independent development or by reason only of reverse engineering, or acquired in the course of the person's work and amounts only to an enhancement of that person's personal knowledge, skill or expertise.

This provision is similar to the US economic espionage offence (18 USC 1831). However, unlike the US, Canada does not have an equivalent to the US theft of trade secrets offence (18 USC 1832). Theft of trade secrets cannot be prosecuted under section 238 of

[93] M. Reid, 'A Comparative Approach To Economic Espionage' 70 (2016) 757 *University Of Miami Law Review* (Reid 2016); Lexis Nexis Article 2012.
[94] Department of Justice, *Chinese Professors Among Six Defendants Charged with Economic Espionage and Theft of Trade Secrets for Benefit of People's Republic of China*, 2015, viewed August 2017, https://www.justice.gov/opa/pr/chinese-professors-among-six-defendants-charged-economic-espionage-and-theft-trade-secrets.
[95] For example, the communication of information by a foreign-owned company operating in Canada does not amount to economic espionage as they have a legitimate commercial right in communicating such information.
[96] Section 22(1), SOI Act.

the Canadian Criminal Code, as theft of property within that section does not include confidential information.[97]

Canada has yet to complete any successful prosecutions for economic espionage.[98] The Royal Canadian Mounted Police (RCMP) has attributed lack of successful prosecutions to the construction of the offence:

- Section 19(1) of the SOI Act requires that theft of trade secrets occurs 'for the benefit or in association of a foreign economic entity'. A foreign economic entity is defined as foreign states or an entity that is controlled by foreign states.[99] Control of an entity by a foreign state has been difficult to prove. For example, the RCMP has been unable to prove that corporations incorporated under Chinese law are subject to control by the state. The RCMP's view is that, for the definition of foreign economic entity to be satisfied the state has to be more than a passive beneficiary and must almost be part of the transaction.
- Section 19(1) further requires that there must be a detriment to Canada's economic interests. The RCMP is of the view that 'detriment' requires major damage to Canada's economy. The RCMP provided a case example where the antigen for a disease found in cows was stolen in Canada. Despite a trade secret being stolen and a company consequently going out of business, the RCMP was unable to indict under economic espionage as the disease was not prevalent in Canada and the theft of the trade secret therefore did not cause a detriment to Canada's economic interests under s19(1) of the SOI Act.
- Defences provided under section 19(3) of the SOI act are misguided and outdated. RCMP observed that is difficult for prosecution to rebut beyond a reasonable doubt, the defence of reverse engineering, which has been a major issue for the RCMP in multiple investigations. Further, the defence of 'acquired in the course of work and amounts to no more than an enhancement of person's knowledge' is too broad and difficult to rebut.

Due to the issues with the economic espionage offence, the RCMP often pursues a breach of trust offence under section 122 of the Canadian Criminal Code.

The Canadian Security Intelligence Service says the long-standing threat of espionage is a worrisome preoccupation for Canada, particularly in relation to Russia and China, who continue to 'target Canada's classified information and advanced technology, as well as government officials and systems'.[100] For example:

---

[97] *R v Stewart* [1988] 1 S.C.R 963 (Can.).
[98] Reid 2016.
[99] Section 2(1) *Security of Information Act* R.S.C., 1985, c. O-5.
[100] J. Bronskill, *Russia, China are out to steal Canada's secrets, spy agency warns*, 2016, viewed August 2017, https://www.thestar.com/news/canada/2016/11/21/russia-china-are-out-to-steal-canadas-secrets-spy-agency-warns.html.

- In 2016, four people, an American, a Briton and two Canadians, were charged with stealing sensitive satellite imaging technology from their employer and selling it to China.[101]
- In 2012, junior Canadian navy officer Jeffrey Delisle was sentenced to 20 years in prison for passing classified western intelligence to Russia in exchange for cash on a regular basis for more than four years. He pleaded guilty to one count of breach of trust and two counts of communicating to a foreign entity under the *Security of Information Act.*[102]
- In 2008 a senior systems security adviser for Nortel Network Corp., discovered that Chinese hackers had been attacking the Canadian company for over a decade and stealing proprietary information.[103]

New Zealand

Section 230 of the *New Zealand Crimes Act 1961* provides a penalty of up to five years imprisonment for dishonestly and without claim of right, taking, obtaining or copying documents, models or any other thing or process, knowing that it contains or embodies a trade secret.[104] There must be intent to obtain any pecuniary advantage or to cause loss to any other person.

'Trade secret' is defined as any information that:

- is or has the potential to be, used industrially or commercially
- is not generally available for commercial use
- has economic value or potential economic value to the possessor of the information and
- is the subject of all reasonable efforts to preserve its secrecy.

Section 230 has yet to be tested through successful prosecutions. The section has rarely been used in indictments and has not been used at all for foreign economic espionage acts.[105]

[101] J.Murphy, *Four charged in Canada with selling stolen satellite equipment to China*. 2016, viewed August 2017, https://www.theguardian.com/world/2016/feb/29/canada-charged-with-selling-stolen-satellite-equipment-china.
[102] S.Chase and J.Taber, *How Canadian spy Jeffrey Delisle betrayed his country for cash,* 2012, viewed August 2017, https://www.theglobeandmail.com/news/politics/how-canadian-spy-jeffrey-delisle-betrayed-his-country-for-cash/article4601092/.
[103] J. Castaldo, *Is industrial espionage putting a chill on foreign investment in Canada?* 2013, viewed August 2017 http://www.canadianbusiness.com/companies-and-industries/spies-like-us/.
[104] A. Kingsbury, 'Trade Secret Crime in New Zealand Law: What Was the Problem and Is Criminalization the Solution?', 37 *European Intellectual Property Review* 147, 149 (2015) (Kingsbury 2015).
[105] Kingsbury 2015 ; Reid 2016.

Foreign Interference

United States

Chapter 45 Title 18, of the US Code contains offences targeting foreign relations, including agents of foreign governments under section 951[106].

Elements of the offence

Section 951 creates a criminal offence for agents of foreign governments who act in the US without first notifying the Attorney General. An agent of a foreign government is defined in subsection 951(d) as an individual who agrees to operate within the US subject to the direction and control of a foreign government or official.[107] The penalty for the offence is a fine, imprisonment of not more than ten years, or both.

Section 951 is often referred to by the US DoJ as 'espionage lite' as it can be used to prosecute information gathering and other espionage-like activities on behalf of a foreign government, including non-political activities, in circumstances where the additional elements constituting espionage offences (such as passage of classified information or an intent to harm the national interest) cannot yet be proved.

Offence in Practice

The US Department of Justice (US Attorney's Office, Southern District of New York) advised that the elements of the offence in section 951 are:

1. The person acted in the US as an agent of a foreign government;
2. The person failed to notify the US AG;
3. The person acted knowingly; i.e. the person knew they had not provided notification to the AG however this does not reach the level of 'willfulness' which requires knowledge of the violation of the law vs knowing the person was acting as an agent.

Section 951 cases generally involve espionage-like or clandestine behaviour or an otherwise provable connection to an intelligence service, or information gathering or procurement-type activity on behalf of a foreign government.

---

[106] Chapter 45 Title 18 also contains offences criminalising: the publication or furnishing of any diplomatic code obtained in the process of transmission between any foreign government and its diplomatic mission in the US (s 952); the purchasing of obligations (etc) of a foreign government while a debt is owed to the US (s 955); conspiring in the US to commit an act outside the US which would constitute murder, kidnapping or maiming if it occurred within US jurisdiction (s 956); and the willful possession or control of property or papers designed or intended to violate any penal statute, where in aid of a foreign government (s 957).

[107] There are exceptions for duly accredited diplomatic and consular officials of foreign governments; any officially and publically acknowledged and sponsored official or representative of a foreign government; officially and publically acknowledged and sponsored member of staff or employee of such an official or representative, who is not a US citizen; and any person engaged in a legal commercial transaction (except if the person is an agent of Cuba or any other country the President determines poses a threat to the US's national security interests, and any specific individual convicted under specific export offences).

The provision has been challenged on constitutional grounds, allegedly violating the right against self-incrimination[108] and has been upheld. The provision was upheld as the statute was concerned only with future acts (one must register prior to becoming agent) and the constitutional protection covers only past activities. In addition, section 951 was held to require all foreign agents to register, even if no future criminal activity is anticipated. The provision has also been challenged as being unconstitutionally vague. The provision was upheld; s951 is a general intent crime that does not require proof that a defendant knew of the notification requirement/ does not require actual notice or knowledge of the notification requirement[109]. Further, the provision has been held as covering 'any affirmative conduct undertaken as an agent of a foreign government' and not merely espionage or traditional spying.[110]

Concerns with the offence

Subsection 951(a) reads "Whoever… acts in the United States as an agent of a foreign government without prior notification to the Attorney-General… shall be fined… or imprisoned…" The subsection can be read to imply that prior notification can absolve a foreign agent of any activity. In practice, no notifications have been received by the Attorney-General.

Secrecy

United States

There are a number of secrecy provisions across the US statute books.[111] These include:

- Title 50 U.S.C. § 783 (Communication of Classified Information by Government Officer or Employee; and Receipt of, or attempt to receive, by foreign agent or member of Communist organization, classified information)
- Title 18 U.S.C. § 793 (Gathering, transmitting or losing defence information)
- Title 18 U.S.C. § 794 (Gathering or delivering defence information to aid foreign government)
- Title 18 U.S.C. § 795 (Photographing and sketching defence installations)
- Title 18 U.S.C. § 797 (Publication and sale of photographs of defence installations)
- Title 18 U.S.C. § 798 (Disclosure of Classified Information); and
- Title 18 U.S.C. § 1924 (Unauthorized Removal and Retention of Classified Documents or Material)

Title 50 – War and National Defence, Chapter 23 – Internal Security

[108] *United States v Melekh* 193 F Supp 586 (NS Ill 1961)
[109] *United States v Duran* 2010
[110] *United States v Duran* 2010
78

Under **paragraph 783(a)** of the *US Code* (Title 50, Chapter 23) it is an offence for a US official[112] to knowingly communicate classified information[113] to another person, who that US official knows, or has reason to believe, is an agent or representative of any foreign government. Similarly, under **paragraph 783(b)** it is offence for any agent or representative of a foreign government to knowingly obtain or receive (or attempt to do so) classified information from a US official, where that person knows, or has reason to know, that the information is classified. The offences do not apply where the disclosure has been specifically authorised by the President or the head of the department/agency/corporation where the US official is employed.

The offences attract a maximum penalty of a fine of US$10,000, ten years' imprisonment, or both. A person must also forfeit any property or proceeds obtained, directly or indirectly, as a result of their offending.

Title 18 – Crimes and Criminal Procedure, Chapter 37 – Espionage and Censorship

Under **section 793** of the *US Code* (Title 18, Chapter 37) it is an offence for a person to gather defence information with intent or reason to believe the information will or could be used to the injury of the US, or to the advantage of a foreign nation. Further to this, persons who have access to defence information that they have reason to know could be used to harm national security, whether the access is authorized or unauthorized, and who disclose that information to any person not entitled to receive it, or wilfully retain the information despite an order to surrender it to an officer of the US, are also committing an offence. It is not necessary that the information be 'classified' by the US Government or a US agency, it is an offence by virtue of the type of information it is.

Offences against section 793 attract a maximum penalty of a fine of US$250,000, ten years' imprisonment, or both. A person must also forfeit any property or proceeds obtained, directly or indirectly, as a result of their offending.

Under **section 794** of the *US Code* (Title 18, Chapter 37) it is an offence for a person to communicate defence information to any foreign government[114], either directly or indirectly, with intent or reason to believe the information will be used to the injury of the US, or to the advantage of a foreign nation. The offence attracts a maximum penalty of life imprisonment, or the death penalty in certain circumstances.[115]

---

[112] The terminology used is 'any officer or employee of the US or of any department or agency thereof, or of any corporation the stock of which is owned in whole or in major part by the US or any department or agency thereof.'
[113] The terminology used is 'any information of a kind which shall have been classified as affected the security of the US.' Section 834 of the Criminal Code (Title 50, Chapter 23) defines 'classified information' as 'information which, for reasons of national security, is specifically designated by a US Government agency for limited or restricted dissemination or distribution.'
[114] 'Or to any faction or party or military or naval force within a foreign country, whether recognised or unrecognised by the US, or to any representative, officer, agent, employee, subject, or citizen thereof.'
[115] Where the disclosure occurs during time of war, with intent that the information reach the enemy; or where the disclosure resulted in the death of a covert agent or directly concerns nuclear weaponry or other sensitive military information (see paragraphs 794(a) and (b)). .

Sections 795 and section 797 of the *US Code* (Title 18, Chapter 37) prohibit the unauthorised creation, publication, sale or transfer of photographs or sketches of vital defence installations or equipment. The maximum penalty for these offences is a fine of US$100,000, one year imprisonment, or both.

Section 798 of the *US Code* (Title 18, Chapter 37) prohibits the unauthorised disclosure of classified information concerning communication intelligence systems and activities. It is an offence for a person to knowingly and wilfully disclose to an 'unauthorised person' any classified information concerning the communication intelligence activities of the US or any foreign government, or obtained by the processes of communication intelligence from the communications of any foreign government.[116] The section also prohibits the use or publication of such information in any manner prejudicial to the safety or interests of the US, or for the benefit of a foreign government to the detriment of the US.

'Unauthorised person' is defined as any person/agency who is not authorised to receive classified information concerning the communication intelligence activities of the US or any foreign government, by the President, or by the head of a department or agency of the US Government which is expressly designated by the President to engage in communication intelligence activities for the US.

The offence attracts a maximum penalty of ten years' imprisonment, a fine of $250,000, or both. A person must also forfeit any property or proceeds obtained, directly or indirectly, as a result of their offending.

Title 18 – Crimes and Criminal Procedure, Chapter 93 – Public officers and employees

Section 1924 of *US Code* (Title 18, Chapter 93) prohibits the unauthorised removal and retention of classified material by officers, employees, contractors or consultants of the US. It is an offence for such persons, by virtue of their position/employment, to knowingly remove documents or materials containing classified information of the US, without authority and with the intent to retain such materials at an unauthorised location.

'Classified information of the US' is defined more broadly than in other sections outlined above. It means 'information originated, owned, or possessed by the US Government concerning the national defence or foreign relations of the US that has been determined pursuant to law or Executive order to require protection against unauthorized disclosure in the interests of national security.'

The offence attracts a maximum penalty of one year imprisonment, a fine of $100,000, or both.

[116] The terminology in the section is 'terminology concerning the nature, preparation, or use of any code, cipher, or cryptographic system of the United States or any foreign government; or concerning the design, construction, use, maintenance, or repair of any device, apparatus, or appliance used or prepared or planned for use by the United States or any foreign government for cryptographic or communication intelligence purposes; or concerning the communication intelligence activities of the United States or any foreign government; or obtained by the processes of communication intelligence from the communications of any foreign government, knowing the same to have been obtained by such processes.

US Case Law

Under Chapter 37 – Espionage and Censorship

US prosecutions of national security leakers (as at May 2014)[117]

Defendant	Subject of leak	Year	Charges	Result
Daniel Ellsberg	The Pentagon Papers	1973	18 U.S.C. §§ 371, 641, 793(c), (d), (e)	Case dropped by prosecutors.
Samuel Morison	Soviet aircraft carrier photos	1985	18 U.S.C. §§ 641, 793(d), (e)	Convicted; sentenced to two years in prison; pardoned in 2001
Lawrence Franklin	U.S. policy toward Iran	2005	18 U.S.C. §§ 371, 793(d), (e), (g); 50 U.S.C. § 783	Pleaded guilty; sentenced to 12 years, reduced to ten months of community confinement
Shamai Leibowitz	Classified information to a blogger	2009	18 U.S.C. § 798(a)	Pleaded guilty; sentenced to 20 months in prison.
Stephen Jin-Woo Kim	Information about North Korea to Fox News	2010	18 U.S.C. §§ 793(d), 1001(a)(2)	Pleaded guilty; sentenced to 13 months in prison.
Thomas Drake	Details of NSA waste and mismanagement	2010	18 U.S.C. §§ 793(e), 1001(a), 1519	Pleaded guilty to misdemeanour in exchange for dropping of more serious charges; sentenced to one year of probation and community service.

[117]Paul Rosenzweig, '*National Security Leaks, Whistle-blowers in the Media*,' (ABA Publishing, 2015), pp. 31-32.

Defendant	Subject of leak	Year	Charges	Result
Bradley (Chelsea) Manning	Massive cache of military and diplomatic files to WikiLeaks	2010	10 U.S.C. §§ 892, 904; 18 U.S.C. §§ 793(e), 1030(a)(1),	Pleaded guilty to ten charges; convicted of 11 additional charges; sentenced to 35 years in prison.
Jeffrey Sterling	Efforts to sabotage Iranian nuclear research to New York Times reporter James Risen	2010	18 U.S.C. §§ 641, 793(d), (e), 1341, 1512(c)(1)	Convicted and sentenced to three years and 6 months in prison.
John Kiriakou	Identity of CIA officials involved in interrogation abuses	2012	18 U.S.C. §§ 793(d), 1001(a)(1); 50 U.S.C. § 421(a)	Pleaded guilty to violating § 421(a); sentenced to 30 months in prison.
James Hitselberger	Classified materials concerning Bahrain to the Hoover Institution	2012	18 U.S.C. §§ 793(e), 2071(a)	Pleaded guilty to misdemeanour in exchange for dropping of more serious charges; sentenced to time already served and fined US$275.

Under Chapter 93 – Public officers and employees

Kristian Saucier – Section 1924 - unauthorised removal and retention of classified records

Saucier, a machinist's mate in the US Navy from 2007-2012, used his mobile phone to take photographs of classified spaces, instruments and equipment of the USS Alexandria (a nuclear attack submarine). Saucier had a secret clearance and knew that the photos depicted classified material and that he was not authorised to take them. Saucier pled guilty to one count of unauthorised removal and retention of classified material. He was sentenced to 12 months' imprisonment, followed by six months of home confinement.

David Petraeus – Section 1924 - unauthorised removal and retention of classified material

A former CIA Director, Petraeus pled guilty in March 2015 to one count of unlawful removal and retention of classified materials under s 1924. He had shared classified information (including Top Secret, code word material) with his biographer and had those documents stored in an unsecured drawer at his home. Petraeus was sentenced to two years' probation, and a fine of US $100,000 ($60,000 more than that proposed, and agreed to by the DoJ, in the plea bargain).

Further detail of offending - During his time as Commander of ISAF in Afghanistan, Petraeus had maintained eight notebooks (black books), including his daily schedule and classified and unclassified notes (including identifies of cover officers, war strategy intelligence capabilities and mechanisms, diplomatic discussions and deliberative discussions from high-level National Security Council meetings). During a conversation with his biographer in 2011, Petraeus was recorded as referencing the black books being 'highly classified' and containing code word information. Several weeks later he agreed to share the black books with her, and later delivered them to a private residence where she was staying (which was not approved for the storage of classified information). He later retrieved the black books and kept them at his residence unapproved.

Bryan Nishimura – Section 1924 - unauthorised removal and retention of classified materials

Nishimura was a naval reservist in Afghanistan (2007-2008), and an engineer for the US military. In 2015 he pled guilty to unauthorised removal and retention of classified materials, for downloading and storing classified information on his personal electronic devices while on tour. He carried the materials with him off-base in Afghanistan and took classified army records to his home, after his deployment ended. In the US, Nishimura continued to maintain the information on unclassified systems. Nishimura's admitted to naval personnel that he had handled classified materials inappropriately and had destroyed a large quantity of classified materials he had maintained in his home. Nishimura was sentenced to two years' probation, fined US$7,500, had his security clearance revoked and was prohibited from seeking a clearance in the future.

John Deutch – various potential offences

Deutch is a former Director of the CIA (1995-1996). After his tenure as Director, classified material was discovered on his personal computer (including Top Secret, code word material). An internal CIA investigation found that he stored and processed hundreds of files of highly classified material on unprotected home computers (or on systems configured for unclassified information only). He and his family used these computers to connect to the Internet, making the information potentially vulnerable to hackers. Formal charges and a prosecution were not originally pursued on an erroneous understanding that Deutch had permission to take the classified material home, and use of the material was permissible in his residence. A subsequent investigation/report by the CIA Inspector General in 2000 found that the security violation occurred when he "did not do it right" by connecting the Internet to his computer and "leaving the card in the slot.' The Inspector-General ultimately recommended Deutch's suitability to retain his security clearance be investigated, and it was ultimately stripped. Deutch was pardoned by President Bill Clinton before the Department of Justice could file any charges.

Canada

Canada's Official Secrets Act was replaced in 2001 by the *Security of Information Act 2001*. The first prosecution under the Security of Information Act took place in 2013, with Sub-Lieutenant Jeffrey Delisle sentenced to 20 years' imprisonment for selling military secrets to Russia.

The offence is similar to offences in sections 70 and 79 of the Australian *Crimes Act 1914* and entails a number of similar problems. The offences in section 4 of the Security of Information Act apply to a broad range of acts, including secrecy, espionage, and offences relating to prohibited places. Section 4 applies where:

- the information was:
    - related to or used in a prohibited place;
    - made or obtained in contravention of the Act (which also includes offences of espionage, economic espionage etc);
    - entrusted in confidence by an officer of the Crown;
    - obtained while the person was subject to the Defence Code of Service Discipline;
    - obtained as a result of the person's position as an officer of the Crown; or
    - obtained as a result of the person's position as a Crown contractor or a contractor working in a prohibited place (or their employee), and
- the person:
    - communicates the information without authorisation or a duty to do so;
    - uses the information for the benefit of any foreign power;
    - uses the information in any manner prejudicial to the safety or interests of the State;
    - unlawfully retains the information
    - fails to comply with lawful directions relating to the return or disposal of the information; or
    - fails to take reasonable care of, or endangers the safety of, the information.

The Act also applies to:

- unlawful receipt of information;
- unlawfully permitting another person to possess information;
- making false statements on applications or declarations; and
- communicating information relating to 'munitions of war' to a foreign power or in any manner prejudicial to the safety or interests of the State.

The SOI Act also provides a regime where particular persons can be permanently bound to secrecy. In those cases, the person commits an offence if they disclose 'special operational information', which includes intelligence and military information, information regarding covert activity, and other sensitive information, regardless of whether that information is true or whether the disclosure would cause harm. This offence is punishable by imprisonment for up to 14 years (for true information) and five years for information regardless of whether it is true. A narrow public interest defence applies.

New Zealand

Section 78A of the *Crimes Act 1961* sets out the offence of wrongful communication, retention or copying of official information. It applies where a person "who owes allegiance to the Sovereign" communicates information likely to prejudice security or defence; retains or copies any official document with the intention to prejudice security or defence; or knowingly fails to comply with lawful directions for the return of an official document relating to security or defence. The maximum penalty is 3 years' imprisonment.

Section 20A of the NZ *Summary Offences Act 1981* also sets out an offence, punishable by up to 3 months' imprisonment or a fine not exceeding $2,000, for other disclosures of official information including where the disclosure is likely to endanger a person's safety, seriously damage the economy, prejudice the maintenance of confidential law enforcement sources, or prejudice the safeguarding of life or property in a disaster or emergency.

The Attorney-General must consent to the filing of charges under each of these offences. There do not appear to have been any prosecutions under these offences.

United Kingdom

The *Official Secrets Act 1989* (1989 Act) contains the UK's unauthorised disclosure offences. There are six categories of information of which disclosure is prohibited:

- security and intelligence
- defence
- international relations
- law enforcement
- foreign confidences, and
- special investigation powers.

The 1989 Act applies different standards to different categories of persons. For instance, any disclosure of information relating to security and intelligence by a current or former employee of the security and intelligence services will constitute an offence, regardless of whether the particular disclosure is damaging. However, current and former Crown Servants and government contractors only commit an offence if their disclosure is damaging.

Members of the public can also be bound by the 1989 Act if they disclose information that was disclosed to them by a Crown Servant or a government contractor without lawful authority, or entrusted to them by a Crown Servant in confidence. It is also an offence for a member of the public to make a damaging disclosure of information relating to security or intelligence, defence or international relations if the information had been

communicated in confidence to another State or international organisation, and the information came into the person's possession without that State or organisation's authority.

The maximum penalty for an unauthorised disclosure under the 1989 Act is two years' imprisonment or an unlimited fine, or both. It is rare for the UK to bring charges for official secrecy under the 1989 Act. While current figures are not publicly available, a 2017 House of Commons Library report indicates that, at least until 2004, fewer than one person per year on average was charged under the 1911 and 1989 Official Secrets Acts, although it is not clear how many of these related to secrecy rather than espionage.

A review by the UK Law Commission of both the espionage and secrecy offences in the Official Secrets Acts. The Law Commission is expected to report later this year.

Sabotage

United States

The US sabotage offences are found in 18 USC Chapter 105 ('Sabotage'). The offences are heavily focused on sabotage of military and national defense property and places, and include:

- wilful trespass, injury or destruction of fortifications, harbor defences, or defensive sea areas;
- destruction of war material, war premises, or war utilities (applies when the US is at war or in a time of national emergency);
- production of defective war material, war premises, or war utilities (applies when the US is at war or in a time of national emergency);
- destruction of 'national-defense materials', 'national-defense premises', or 'national-defense utilities'; and
- production of defective national-defense material, national-defense premises, or national-defense utilities.

Prosecutions in the US are more frequent for the offence of sabotage as compared to other offences being considered by the review (eg. sedition, treason). US prosecutions have covered the following types of conduct:

- nuclear protestors intentionally damaging missile sites (including damaging radar devices, electrical cables, locks controlling access to the missiles, and concrete launch lid)[118]
- throwing a bolt into an engine intake of an aircraft[119]

[118] See U*.S. v Kabat* (1986) 797 F. 2d 580. Two defendants were sentenced to nine years plus restitution on the sabotage count, another to a sentence of five years, and another to a sentence of four years.
[119] See *U.S. v Johnson* (1987) 24 M.J. 101. In this case the court held that the term 'intent' in the sabotage provisions means knowing that the result is practically certain to follow, regardless of any desire, purpose or motive

- destruction of high-voltage electric line towers for the purpose of creating domestic turmoil[120], and
- throwing flaming objects at an air force building on a university campus.[121]

Canada

Section 52 of the Canadian *Criminal Code* sets out the offence of sabotage, which occurs when a person does a 'prohibited act' for a purpose prejudicial to the safety, security or defence of Canada, or the safety or security of the defence forces of any other state that are lawfully present in Canada. A 'prohibited act' means an act or omission that impairs the efficiency or impedes the working of any vessel, vehicle, aircraft, machinery, apparatus or other thing, or causes property to be lost, damaged or destroyed. Exceptions apply for industrial disputes and door-to-door canvassing. The offence attracts a maximum penalty of 10 years' imprisonment.

In 2009, two military officers were charged with sabotage after compromising a classified government computer system (the system took around 4 hours to fix).

New Zealand

Section 79 of the New Zealand *Crimes Act 1961* sets out an offence similar to the Canadian offence of sabotage. It prohibits any act that impairs the efficiency or impedes the working of any ship, vehicle, aircraft, arms, munitions, equipment, machinery, apparatus, or atomic or nuclear plant; or damages or destroys any property which it is necessary to keep intact for the safety or health of the public. The offence applies when the acts are done with intent to prejudice the safety, security or defence of New Zealand or the safety or security of the armed forces of any other country lawfully present in New Zealand. The maximum penalty is 10 years' imprisonment. Strikes and lockouts are expressly excluded.

Those involved in mining the Rainbow Warrior were charged with murder, conspiracy and arson, as opposed to sabotage.

United Kingdom

The UK does not have any specific sabotage offences. However, section 1 of the *Official Secrets Act 1911* has been interpreted as including sabotage. As well as preventing the unauthorised gathering or communication of information, section 1 prohibits approaching, inspecting or entering (etc) any 'prohibited place' for any purpose prejudicial to the safety or interests of the State. This interpretation was used in 1964 to prosecute supporters of

---

to achieve that result. As such, the offence is made out if someone acted when he knows injury to national defence is inevitable, even though their reason for acting has nothing to do with national defence.

[120] See *U.S. v Bishop* (1977) 555 F.2d 771.

[121] See *U.S. v Eisenberg* (1972) 469 F.2d 156.

the Campaign for Nuclear Disarmament, who attempted to immobilise a defence air base and reclaim it for civil purposes.[122]

Although the Official Secrets Acts are being reviewed, the Law Commission's consultation paper only briefly mentions sabotage and makes a provisional conclusion that an offence should continue to apply to those who inspect, pass over or enter any prohibited place.

Treason

United States

Treason is defined in Article 3, section 3 of the *US Constitution* as 'levying War against them [the US], or in adhering to their [US] Enemies, giving them Aid and Comfort.' Section 3 further provides that 'no person can be convicted of treason unless there is the testimony of two witnesses to the same overt act, or on confession in an open court.'

The offence of *Treason* is found under Title 18, Chapter 115, section 2381 of the *United States Criminal Code*. It is an offence for a person owing allegiance to the United States,[123] to levy war against the US or adhere to their enemies, giving them aid and comfort within the US or elsewhere. The penalty for this offence is:

- the death penalty, or
- imprisonment of not less than five years AND a fine of not less than $10,000.

In addition to the above penalties, a person shall be incapable of holding any United States public office.

Section 2382 sets out the offence of 'Misprision of Treason', which in essence criminalises concealing the offence of treason. It is an offence for a person, who knows that an offence of treason has been committed, to conceal or otherwise not disclose the fact that a treason offence has been committed. The person must disclose this to the President, a Judge, Governor or Justice of a State. This offence is punishable by a fine and/or a maximum period of imprisonment of seven years.

Canada

Section 46(1) of the Canadian *Criminal Code 1985* defines the offence of 'high treason'. It is an offence, punishable by life imprisonment, for any person to do any of the following in Canada:

- kill, attempt to kill, do bodily harm tending to death or destruction, maim, wound, imprison or restrain Her Majesty, or
- levy war against Canada or do any preparatory acts, or

---

[122] *Chandler and others v Director of Public Prosecutions* [1964] AC 763; [1962] 3 WLR 694.
[123] The concept of owing allegiance to the US is not defined in the Criminal Code.

- assist an enemy at war with Canada, or any armed forces engaged in hostilities with Canada, whether or not a state of war exists between them.

Section 46(2) of the *Criminal Code* contains the offence of 'treason'. It is an offence for any person to do any of the following in Canada:

(a) use force or violence for the purpose of overthrowing Canadian government, conspire to do so or form an intent to do so and manifest that intention by an overt act. This offence is punishable by life imprisonment.
(b) without lawful authority communicate or make available to an agent[124] of a foreign state, military or scientific information[125] that they know or ought to know may be used for a purpose prejudicial to the safety or defence of Canada, conspire to do so or form an intent to do so and manifest that intention by an overt act. This offence is punishable by life imprisonment when a state of war exists between Canada and another country. Where there is no state of war, the offence is punishable by a maximum of 14 years' imprisonment.
(c) form an intention to commit high treason (as established under s46(1)) and manifest that intention by an overt act. This is punishable by life imprisonment.

Subsection 46(3) of the *Criminal Code* extends these offences to conduct that occurs outside of Canada, where the person is a Canadian citizen or owes allegiance to Canada. Subsection 47(3) provides that no conviction for treason can be established on the evidence of only one witness, unless the evidence of that witness is corroborated by other material.

Paragraph 46(2)(b) (unlawfully sharing military or scientific information with an agent of a foreign state) perhaps provides the biggest distinction between Canada and Australia/the US. Here, it appears that conduct amounting to treason overlaps with conduct more traditionally associated with espionage, especially as the legislation is framed in a way that indicates a state of war does not have to exist specifically with the country that the military/scientific information is supplied to.

As a comparison, the espionage provisions under Canada's *Security of Information Act 1985* (SOI Act) make it an offence to communicate 'safeguarded' or 'special operational' information to a foreign entity without lawful authority. 'Special operational information" is defined in section 8 of the SOI Act as information that the Government of Canada is taking measures to safeguard that reveals, or from which may be inferred:

- the identity of a person, agency, group, body or entity which is, or is intended to be, a confidential source of information, intelligence or assistance to the Government
- nature or content of plans for military operations in respect of armed conflict

[124] 'Agent' is not defined in the Criminal Code.
[125] 'Military or scientific information' is not defined in the Criminal Code. The term 'military' is defined in section 1 as 'relating to all or any of the Canadian forces.'

- means used, intended to be used, or capable of being used to covertly collect, obtain, decipher, assess, analyse, communicate or otherwise deal with information or intelligence
- whether a place, person, agency, group, body or entity was/will be the object of a covert investigation
- means used, or capable of being used, by the Government to protect or exploit the above information/intelligence
- information or intelligence similar in nature to the information referred to above, that is in relation to, or received from, a foreign entity or terrorist group.

Section 50(1)(b) of the *Criminal Code* makes it an offence to know that a person is about to commit high treason or treason and fail to inform a justice of the peace or other peace officer,[126] or otherwise take reasonable efforts to prevent such acts. This offence is punishable by a maximum of 14 years' imprisonment.

Interestingly, the Canadian treason offences apply to 'every one' who commits the defined conduct in subsections 46(1) and (2) – there are not the same citizenship/residency requirements that exist under Australian law (which were specifically inserted when the offences were amended in 2010). Canadian citizens and persons owing allegiance to Her Majesty in right of Canada and who commit acts of high treason or treason are punishable under Canadian criminal law even if the acts were performed outside of Canada.

Commentary on the application of Canada's treason offences note that while they appear to be framed broadly, there is a general reluctance to charge perpetrators with the offence of treason[127].

United Kingdom

Treason offences in the UK rely on archaic statutes[128] criminalising the following acts, punishable by life imprisonment:

- plotting the murder of the sovereign
- 'violating' the sovereign's companion, eldest unmarried daughter or the wife of the heir to the throne

---

[126] 'Peace officer' is broadly defined in section 2 of Canada's Criminal Cod, and includes a mayor, warden, sheriff, member of the Correctional Service of Canada who is designated as a peace officer, a police officer, police constable, bailiff, constable, customs officer, fishery guardian, pilot and officers of the Canadian forces.

[127] Enforcement Agencies, charge alternative offences to treason. In *R v Alizadeh,* 2014 ONSC 5421, the defendant was not charged with treason offences, despite the judge commenting in sentencing proceedings that 'you have effectively been convicted of treason'. He was instead prosecuted for possessing explosive materials for the purpose of endangering life/causing serious property damage. In another example, the perpetrators of the Toronto 18 terrorist plot in 2006 were charged with terrorism offences when arguably their actions were treasonous.

[128] Section II *Treason Act 1351; Treason Felony Act 1848* and *Treason Act 1702.* These treason offences apply to England, Scotland (by virtue of the *Treason Act 1708*) and Northern Ireland (by virtue of *The Treason Act (Ireland) 1537* and *Crown of Ireland Act 1542.* Section 36 of the *Crime and Disorder Act 1998* introduced a maximum penalty of life imprisonment for these offences, abolishing the death penalty which previously applied.

- levying war against the sovereign, adhering to the sovereign enemies, giving them aid and comfort
- killing a sovereign's chancellor, treasurer or Justices
- endeavouring to undermine the lawful line of succession, and
- using force or constraint to compel the Crown regarding their measures or counsels, in order to intimidate or overthrow both or either House of Parliament.

The last treason case in the UK was that of William Joyce, who was convicted of 'adherence to the King's enemies' and executed for broadcasting Nazi propaganda to the UK during World War II[129].

New Zealand

Section 73 of New Zealand's *Crimes Act 1961* deals with the act of treason, which is defined as:

- killing, wounding or doing grievous bodily harm to the sovereign,
- imprisoning or restraining the sovereign,
- levying war against New Zealand,
- assisting an enemy at war with New Zealand or any armed forces against which New Zealand forces are engaged in hostilities with (whether or not a state of war exists between New Zealand and any other country),
- inciting or assisting any person with force to invade New Zealand, or
- conspiring with any person to do any of the above acts.

All of the above, with the exception of conspiring to commit treason, are punishable by life imprisonment (ss 74(1)). The offence of conspiracy to commit treason is punishable by a maximum of 14 years' imprisonment (ss 74(2)), as is attempt to commit treason (either within or outside of New Zealand) (ss 74(3)).

In order for the treason provisions to apply, the person engaging in the relevant conduct must owe an allegiance to the Sovereign in right of New Zealand. Subsection 75(1) provides that no one can be convicted of treason on the evidence of one witness only, unless evidence of the witness is corroborated in some material particular by evidence implicating the defendant. However this subsection does not apply to an act where the sovereign is killed or wounded (as per ss 73(a)).

New Zealand also has an offence of being a party to treason, which is punishable by a maximum term of 7 years' imprisonment. The offence applies to a person who has become an accessory after the fact to treason or to knowing that a person is about to commit treason and failing to inform a constable as soon as possible, or to use other reasonable efforts to prevent its commission.

[129] *R v Joyce* [1946] A.C 347.

Appendix C – Comparison of old and new offences

NEW OFFENCE	NEW SECTION – CRIMINAL CODE ACT 1995 (CTH)	PENALTY	PREVIOUS CRIMINAL OFFENCE AND PENALTY
ESPIONAGE AND THEFT OF TRADE SECRETS			
Espionage			
Espionage—dealing with information concerning national security which is or will be made available to foreign principal – intention as to national security	Subsection 91.1(1)	Life	Section 91.1 Criminal Code Act 1995 (*Espionage and similar activities*), punishable by 25 years imprisonment
Espionage—dealing with information concerning national security which is or will be made available to foreign principal – reckless as to national security	Subsection 91.1(2)	25 years	
Espionage—dealing with information which is or will be made available to foreign principal – intention as to national security	Subsection 91.2(1)	25 years	
Espionage—dealing with information which is or will be made available to foreign principal– reckless as to national security	Subsection 91.2(2)	20 years	
Espionage—security classified information etc.	Section 91.3	20 years	
Espionage on behalf of a foreign principal			
Espionage on behalf of foreign principal – intention as to national security	Subsection 91.8(1)	25 years	
Espionage on behalf of foreign principal – reckless as to national security	Subsection 91.8(2)	20 years	

NEW OFFENCE	NEW SECTION – CRIMINAL CODE ACT 1995 (CTH)	PENALTY	PREVIOUS CRIMINAL OFFENCE AND PENALTY
Espionage on behalf of foreign principal – conduct on behalf of foreign principal	Subsection 91.8(3)	15 years	
Espionage - related offences			
Offence of soliciting or procuring an espionage offence or making it easier to do so	Section 91.11	15 years	
Offence of preparing for an espionage offence	Section 91.12	15 years	
Theft of trade secrets involving foreign government principal (economic espionage)			
Theft of trade secrets involving foreign government principal	Section 92A.1	15 years	
FOREIGN INTERFERENCE			
Intentional foreign interference – interference generally	Subsection 92.2(1)	20 years	
Intentional foreign interference– interference involving targeted person	Subsection 92.2(2)	20 years	
Reckless foreign interference – interference generally	Subsection 92.3(1)	15 years	
Reckless foreign interference – interference involving targeted person	Subsection 92.3(2)	15 years	
Foreign interference - related offences			
Preparing for a foreign interference offence	Section 92.4	10 years	
Knowingly supporting a foreign intelligence agency	Section 92.7	15 years	

NEW OFFENCE	NEW SECTION – CRIMINAL CODE ACT 1995 (CTH)	PENALTY	PREVIOUS CRIMINAL OFFENCE AND PENALTY
Recklessly supporting a foreign intelligence agency	Section 92.8	10 years	
Knowingly funding or being funded by a foreign intelligence agency	Section 92.9	15 years	
Recklessly funding or being funded by a foreign intelligence agency	Section 92.10	10 years	
SECRECY OF INFORMATION			
Inherently harmful information			
Communication of inherently harmful information	Subsection 122.1(1)	15 years	Paragraph 79(2)(a) Crimes Act 1914 (*Official secrets*), punishable by 7 years imprisonment
Other dealings with inherently harmful information	Subsection 122.1(2)	5 years	
Inherently harmful information removed from, or held outside, proper place of custody	Subsection 122.1(3)	5 years	
Failure to comply with lawful direction regarding inherently harmful information	Subsection 122.1(4)	5 years	
Information causing harm to Australia's interests			
Communication causing harm to Australia's interests	Subsection 122.2(1)	15 years	Section 79 Crimes Act 1914 (*Official secrets*), punishable by 6 months to 7 years imprisonment
Other conduct causing harm to Australia's interests	Subsection 122.2(2)	5 years	

NEW OFFENCE	NEW SECTION – CRIMINAL CODE ACT 1995 (CTH)	PENALTY	PREVIOUS CRIMINAL OFFENCE AND PENALTY
Information removed from, or held outside, proper place of custody causing harm to Australia's interests	Subsection 122.2(3)	5 years	
Failure to comply with direction regarding information causing harm to Australia's interests	Subsection 122.2(4)	5 years	
Unauthorised disclosure by Commonwealth officer			
Unauthorised disclosure of information by Commonwealth officers	Subsection 122.4(1)	2 years	Section 70 Crimes Act 1914 (*Disclosure of information by Commonwealth officers),* punishable by 2 years imprisonment
SABOTAGE			
Sabotage involving foreign principal with intention as to national security	Section 82.3	25 years	
Sabotage involving foreign principal reckless as to national security	Section 82.4	20 years	
Sabotage with intention as to national security	Section 82.5	20 years	Section 24AB Crimes Act 1914 (*Sabotage*), punishable by 15 years imprisonment
Sabotage reckless as to national security	Section 82.6	15 years	
Sabotage - related offences			
Introducing vulnerability with intention as to national security	Section 82.7	15 years	

NEW OFFENCE	NEW SECTION – CRIMINAL CODE ACT 1995 (CTH)	PENALTY	PREVIOUS CRIMINAL OFFENCE AND PENALTY
Introducing vulnerability reckless as to national security	Section 82.8	10 years	
Preparing for or planning sabotage	Section 82.9	7 years	
TREASON AND TREACHERY			
Treason—assisting enemy to engage in armed conflict	Section 80.1AA	Life	Section 80.1AA Criminal Code Act 1995 (*Treason—materially assisting enemies etc.)*, punishable by life imprisonment
Treachery	Section 80.1AC	Life	Section 24AA Crimes Act 1914 (*Treachery)*, punishable by life imprisonment
OTHER THREATS AGAINST SECURITY			
Advocating mutiny	Section 83.1	7 years	Section 25 Crimes Act 1914 (*Inciting Mutiny)*, punishable by life imprisonment
Assisting prisoners of war to escape	Section 83.2	15 years	Section 26 Crimes Act 1914 (*Assisting prisoners of war to escape)*, punishable by life imprisonment
Military-style training involving foreign government principal	Section 83.3	20 years	Section 27 Crimes Act 1914 (*Unlawful drilling)*, punishable by 5 years imprisonment

NEW OFFENCE	NEW SECTION – CRIMINAL CODE ACT 1995 (CTH)	PENALTY	PREVIOUS CRIMINAL OFFENCE AND PENALTY
Interference with political rights and duties	Section 83.4	10 years	Section 28 Crimes Act 1914 (*Interfering with political liberty*), punishable by 3 years imprisonment
FALSE OR MISLEADING INFORMATION			
Aggravated offence for giving false or misleading information	Section 137.1A	5 years	
DAMAGING COMMONWEALTH PROPERTY			
Damaging Commonwealth property	Section 132.8A	10 years	Section 29 Crimes Act 1914 (*Destroying or damaging Commonwealth property*), punishable by 10 years imprisonment