PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

Advisory Report on the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017

Parliamentary Joint Committee on Intelligence and Security

June 2018
CANBERRA

© Commonwealth of Australia

ISBN 978-1-74366-830-6 (Printed Version)

ISBN 978-1-74366-831-3 (HTML Version)

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Australia License.

The details of this licence are available on the Creative Commons website: http://creativecommons.org/licenses/by-nc-nd/3.0/au/.

Contents

Membership of the Committee xi

Terms of Reference xiii

List of Abbreviations xv

List of Recommendations xvii

The Report

1 Current environment 1

The current environment 1

Government response to the threat 6

Committee comment 9

2 The Bill and its referral 11

The Bill and its referral 11

Objectives of the Bill 11

Conduct of the inquiry 13

Report structure 14

Outline of the Bill 15

Schedule 1- Treason, espionage, foreign interference and related offences ... 16

Schedule 2 – Secrecy 22

Schedule 3 – Aggravated offence for giving false or misleading information 24

Schedule 4 - Telecommunications serious offences 24

Schedule 5 - Foreign Influence Transparency Scheme 25

3 General issues across the Bill 27

Scope of key definitions 27

Definition of 'national security' 27

'Prejudice' and 'advantage' of national security 37

Definition of 'foreign principal' 40

Definition of 'foreign intelligence agency' 43

Definition of 'Australian Government security clearance' 45

Secrecy-related definitions 46

Committee comment 47

Security classifications 52

Regulations 53

Appropriateness as a threshold for criminality 57

Strict liability 62

Evidentiary certificates 66

Government proposed amendments 70

Committee comment 72

Evidentiary certificates - 'concerns national security' 76

Committee Comment 78

Preparatory offences 79

Committee comment 82

Reckless conduct 83

Committee comment 84

Evidential burden on the defendant 84

Rights to freedom of expression and political communication 90

4 Secrecy offences - breadth of conduct captured 95

Overview of the provisions 95

Rationale for the proposed new offences 98

Australian Law Reform Commission report 101

Breadth of conduct captured by the offences 105

Breadth of 'deal with' offences 106
Breadth of 'inherently harmful information' offences 109
Breadth of 'cause harm to Australia's interests' offences 117
'Proper place of custody' offences 125
'Lawful direction' offences 126
Aggravated offences 129
Application to 'insiders' and 'outsiders' 131
Consistency with freedom of information laws 136
Replication of section 70 of the Crimes Act 138
Freedom of expression and political communication 141
Committee comment 144

5 Secrecy offences - defences and other matters 155

Defences 155
Official duties – subsection 122.5(1) 155
Oversight bodies, courts and tribunals – subsections 122.5(3)–(5) 162
Journalists and their associates – subsection 122.5(6)–(7) 165
External whistleblowers 172
Information that has been previously communicated or made public – subsections 122.5(2) and (8) 175
Information relating to a person – subsection 122.5(9) 179
Legal advice 180
Committee comment 181
Other matters 188
Interactions with other legislation 188
Penalties 193
Attorney-General's consent to institute proceedings 195
Consequential amendments 196
Committee Comment 197

6 Espionage offences 201

Overview of the provisions 201
Rationale for the proposed new offences 203
Subdivision A – Espionage 205
Meaning of 'made available' to a foreign principal 207
Breadth of definitions of 'national security' 'foreign principal' and 'deals' 208
Breadth of information captured 212
Fault elements 217
Extra-territoriality and sovereignty 220
Aggravated offences 221
Government proposed amendments 223
Subdivision B – Espionage on behalf of foreign principal 224
Subdivision C – Espionage-related offences 225
Soliciting, procuring and making it easier to commit espionage 226
Preparing for espionage 228
Defences 228
Exposure to liability – public officials and allies 231
Consistency with secrecy defences 233
Penalties 234
Proportionality 234
Freedom of political communication and expression 235
Attorney-General's Consent 238
Consequential amendments 239
Citizenship 239
Presumption against bail 239
Standard non-parole periods 239
Committee Comment 239
7 Foreign interference and theft of trade secrets offences 247
Foreign interference offences 247
Rationale for the new offences 248

General foreign interference offences 249
Offences involving foreign intelligence agencies 253
Defences 258
Interaction with the Foreign Influence Transparency Scheme Bill 2017 260
Consequential amendments 261
Committee comment 262
Theft of trade secrets 264
Overview of the offence 264
Rationale for the new offence 266
Penalty 269
Defences 269
Attorney-General's Consent 269
Civil versus criminal enforcement 269
Committee Comment 271
8 Sabotage offences 273
Definitions of 'damage to public infrastructure' and 'public infrastructure' 274
Critical infrastructure versus public infrastructure 277
Intention and recklessness as to national security 278
Harm or prejudice to Australia's economic interests, and other matters 280
Preparing for or planning a sabotage offence 281
Penalties 282
Defences 283
Consequential amendments 286
Telecommunications interception 286
Citizenship 286
Deportation 286
Committee comment 286
9 Treason, treachery and other threats to security 289
Treason and treachery 290

Treason 290
Treachery 295
Committee comment 299
Other threats to security 300
Consequential amendments 301
Advocating mutiny 301
Assisting prisoners of war to escape 304
Military style training involving foreign government principal 305
Interference with political rights and duties 309
Damaging Commonwealth property 311
Committee comment 313
10 Schedules 3 to 5 and consequential amendments 319
Schedule 3 – Aggravated offence for giving false or misleading information 320
Scope of the offence 320
Definition of key terms 322
Defences 322
Telecommunications interception 322
Committee Comment 322
Schedule 4 – Telecommunications interception 324
Application to aggravated offence of providing misleading information and secrecy offences 325
Committee Comment 327
Schedule 5 – The Foreign Influence Transparency Scheme Bill 2017 329
Committee comment 330
Consequential amendments 331
Cessation of citizenship 331
Citizenship applications 335
Deportation 338
Presumption against bail 339

In-camera proceedings 345

Standard non-parole periods 347

11 Concluding comments 351

Appendix A. List of submissions and exhibits 353

Appendix B. List of witnesses appearing at public and private hearings 357

Appendix C. Comparison between Schedule 2 and ALRC recommendations ... 363

Membership of the Committee

Chair

Mr Andrew Hastie MP

Deputy Chair

Hon Anthony Byrne MP

Members

Hon Mark Dreyfus QC, MP

Hon Dr Mike Kelly AM, MP

Mr Julian Leeser MP

Mr Jason Wood MP

Senator the Hon Eric Abetz (from 7/2/18)

Senator David Bushby

Senator David Fawcett

Senator Jenny McAllister

Senator Bridget McKenzie (to 20/12/17)

Senator the Hon Penny Wong

Terms of Reference

On 8 December 2017, the Prime Minister referred the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 to the Committee for inquiry and report.

List of Abbreviations

AFP	Australian Federal Police
AGSVA	Australian Government Security Vetting Agency
ALRC	Australian Law Reform Commission
ASIO	Australian Security Intelligence Organisation
ASIO Act	*Australian Security Intelligence Organisation Act 1979* (Cth)
the Bill	National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017
Crimes Act	*Crimes Act 1914* (Cth)
FITS Bill	Foreign Influence Transparency Scheme Bill 2017
FOI Act	*Freedom of Information Act 1982* (Cth)
the Guide	*Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*
ICCPR	International Covenant on Civil and Political Rights
IGIS	Inspector-General of Intelligence and Security
IGIS Act	*Inspector-General of Intelligence and Security Act 1986* (Cth)
JSCEM	Joint Standing Committee on Electoral Matters

NSI Act	*National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth)
Ombudsman Act	*Ombudsman Act 1976* (Cth)
PID Act	*Public Interest Disclosure Act 2013* (Cth)
POCA	*Proceeds of Crime Act 2002* (Cth)
Privacy Act	*Privacy Act 1988* (Cth)
TIA Act	*Telecommunications (Interception and Access) Act 1979*(Cth)

List of Recommendations

Recommendation 1

1.29 The Committee recommends that, following implementation of the recommendations in this report, the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 be passed.

Recommendation 2

3.73 The Committee recommends that the Bill be amended to clarify that, for the purpose of the Bill's espionage, foreign interference and sabotage offences, the expression 'prejudice to national security' cannot consist of

- embarrassment alone, and
- must also include a degree of damage or harm.

Recommendation 3

3.76 The Committee recommends that the Bill be amended to reflect the intent of the Explanatory Memorandum that the term 'advantage the national security of a foreign country' does not apply to conduct that is mutually advantageous to the security of both Australia and the foreign country.

Recommendation 4

3.81 The Committee recommends that the Explanatory Memorandum be amended to provide greater clarity about the intended meaning of the terms 'espionage', 'sabotage', 'political violence' and 'foreign interference' for the purposes of the definition of national security at proposed section 90.4.

Recommendation 5

3.83 The Committee recommends that the Bill be amended to clarify that the Bill does not affect the operation of existing provisions in the *Australian Security Intelligence Organisation Act 1979*, unless explicitly stated.

Recommendation 6

3.88 The Committee recommends that the Bill be amended to define what foreign political organisations may be covered by the term 'foreign political organisation'.

Recommendation 7

3.94 The Committee recommends that the Bill be amended to define the meaning of 'Australian Government security clearance'.

Recommendation 8

3.167 The Committee recommends that the Bill be amended to define each 'security classification' to which criminal liability attaches. Each definition should include harm-based statutory criteria for determining the proper classification to apply to that information. Any material incorporated by reference into the regulations should be required to be publicly available.

Recommendation 9

3.168 The Committee recommends implementing the Attorney-General's proposed amendments to

- narrow the proposed definition of 'security classification' to a classification of SECRET or TOP SECRET, or equivalent, and
- remove strict liability from espionage and secrecy offences.

Recommendation 10

3.169 The Committee recommends that the Bill be amended to require that, prior to initiating proceedings for an espionage or secrecy offence that relies on the fact that information is security classified, the head of the originating agency must certify that it is appropriate that the information had a security

classification at the time of the conduct that is alleged to constitute the offence.

This certificate should operate as a condition precedent to the initiation of proceedings. The certificate should not have any evidentiary effect.

Recommendation 11

3.170 The Committee recommends that the Bill be amended to remove the evidentiary certificate regimes in proposed sections 93.3(1)(a)-(b) and 121.3, in relation to security classified information.

Recommendation 12

3.178 The Committee recommends that the Bill be amended to remove the evidentiary certificate regimes in proposed sections 93.3(1)(c)-(d), in relation to information that 'concerns Australia's national security'.

Recommendation 13

3.192 The Committee recommends that the Government amend the *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* to identify criteria to be used for determining the kinds of criminal conduct that warrant preparatory offences.

Recommendation 14

4.156 The Committee recommends that the Bill include a note making explicit that the secrecy offences relating to security classified information and other 'inherently harmful information' will only apply where a person intentionally deals with the relevant information, and where the person is reckless as to the nature of that information.

Recommendation 15

4.160 The Committee recommends that the Attorney-General's proposed amendments to narrow the scope of the offences at proposed section 122.1 in relation to 'inherently harmful information' be implemented. This includes removing paragraph (d) from the definition of 'inherently harmful information', removing strict liability from elements of the offences, and limiting the offences to Commonwealth officers.

Recommendation 16

4.161 The Committee recommends that the Bill be amended to move paragraph (b)—information the communication of which would, or could be reasonably expected to, damage the security or defence of Australia—from the definition of 'inherently harmful information' into the definition of 'cause harm to Australia's interests' in proposed section 121.1.

Recommendation 17

4.165 The Committee recommends that the Attorney-General's proposed amendments to narrow the scope of the offences at proposed section 122.2 in relation to conduct causing harm to Australia's interests be implemented. This includes removing paragraphs (a)(i), (d) and (e) from the definition of 'cause harm to Australia's interests', clarifying that paragraph (f) applies to the health or safety of the *Australian* public, or a section of the *Australian* public, and limiting the offences to Commonwealth officers.

Recommendation 18

4.167 The Committee recommends that the Bill be amended to require that any material incorporated into regulations for the purpose of the definition of 'proper place of custody' at proposed section 121.2 be publicly available.

Recommendation 19

4.170 The Committee recommends that the Bill be amended to limit the secrecy offence at proposed section 122.1(4), in relation to failing to comply with a lawful direction, to directions that have been issued for the purpose of protecting the security of the 'inherently harmful information' against unauthorised access or disclosure.

Recommendation 20

4.175 The Committee recommends that the Bill be amended to limit the aggravating factor at subparagraph 122.3(1)(b)(v), in relation to the proposed secrecy offences for Commonwealth officers, to persons holding an Australian Government security clearance that allows the person to access information with a classification of SECRET or above.

Recommendation 21

4.179 The Committee recommends that the Attorney-General's proposed amendments, to create separate secrecy offences that apply to non-Commonwealth officers that are narrower in scope than those applying to Commonwealth officers, be implemented.

Recommendation 22

4.183 The Committee recommends that the Bill be amended to make clear the effect of the defences in subsections 122.5(1) and (2) in relation to the *Freedom of Information Act 1982*.

Recommendation 23

4.187 The Committee recommends that the Bill be amended to apply a sunset period of five years to proposed section 122.4 ('Unauthorised disclosure of information by current and former Commonwealth officers etc.').

Recommendation 24

4.190 The Committee recommends that, following the passage of the general secrecy offences in Schedule 2 to the Bill, the Attorney-General initiate a review of existing secrecy offences contained in other legislation, taking into account the set of principles contained in the Australia Law Reform Commission's report, *Secrecy Laws and Open Government in Australia*.

Recommendation 25

5.85 The Committee recommends that the Bill be amended to ensure that staff of the Inspector-General of Intelligence and Security are appropriately protected, noting the limitations on the Inspector-General and members of staff of the Inspector-General giving evidence under the *Inspector-General of Intelligence and Security Act 1986*. The Committee recommends that this amendment be developed in consultation with the Inspector-General and her Office.

Recommendation 26

5.87 The Committee recommends that the following proposed defences be broadened to cover all dealings with information, rather than being limited to communication of information:

- proposed section 122.5(3) – relating to the Inspector-General of Intelligence and Security, the Commonwealth Ombudsman and the Law Enforcement Integrity Commissioner,

- proposed section 122.5(4) – relating to the *Public Interest Disclosure Act 2013*,

- proposed section 122.5(5) – relating information provided to a court or tribunal, and

- proposed section 122.5(8) – relating to information that has been previously communicated.

Recommendation 27

5.90 The Committee recommends that the Attorney-General's proposed amendments to the defence for journalists at proposed section 122.5(6), and the associated amendments at 122.5(7), be implemented. This includes expanding the defence to all persons engaged in reporting news, presenting current affairs or expressing editorial content in news media where the person reasonably believed that dealing with or holding the information was in the public interest.

The Committee also recommends that the Government consider further refinements to the proposed defence in order to

- make explicit that editorial support staff are covered by the defence, including legal advisors and administrative staff,

- ensure editorial staff and lawyers, who are engaging with the substance of the information, be required to hold a reasonable belief that their conduct is in the public interest, and

- allow administrative support staff working at the direction of a journalist, editor or lawyer who holds the reasonable belief, to benefit from the defence.

Recommendation 28

5.95 The Committee recommends that the Bill be amended to remove proposed paragraph 122.5(7)(d), which currently limits the availability of the defence for persons engaged in reporting news.

Recommendation 29

5.104 The Committee recommends that the Bill be amended to provide for a defence for a person who reports, to an appropriate entity, malpractice or maladministration in the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth or the functions of the Australian Federal Police under paragraph 8(1)(be) of the *Australian Federal Police Act 1979* or the *Proceeds of Crimes Act 2002*.

Recommendation 30

5.106 The Committee recommends that the Bill be amended to include a defence for dealing with information for the purpose of obtaining legal advice.

Recommendation 31

5.137 The Committee recommends that the Bill be amended to clarify that the secrecy offences in Schedule 2 do not override the obligations and immunities included in the:

- *Freedom of Information Act 1982*,
- *Privacy Act 1988*,
- *Ombudsman Act 1976*,
- *Inspector-General of Intelligence and Security Act 1986*, or
- *Public Interest Disclosure Act 2013*.

Recommendation 32

5.138 The Committee recommends that the *Inspector-General of Intelligence and Security Act 1986* be amended to extend statutory immunity to persons who voluntarily provide information to the Inspector-General or her office.

Recommendation 33

5.141 The Committee recommends that Bill be amended to require the Attorney General's consent for a prosecution under the proposed secrecy offences in Division 122 of the Bill. In deciding whether to consent, the Attorney-General should be required to consider whether the conduct might have been authorised or is otherwise covered by an exception under any of the proposed defences in the Division.

Recommendation 34

5.144 Consistent with recommendations of the Australian Law Reform Commission, the Committee recommends that the Bill be amended to reduce the maximum penalty for the secrecy offences in proposed sections 122.1, 122.2 and 122.4A to seven years' imprisonment for conduct involving communication of information, and three years' imprisonment for other dealings.

The maximum penalty for the aggravated secrecy offences in proposed section 122.3 should be ten years' imprisonment for conduct involving communication of information (consistent with the most serious secrecy offences in the *Australian Security Intelligence Organisation Act 1979* and the *Intelligence Services Act 2001*), and five years' for other dealings.

Recommendation 35

6.151 The Committee recommends that the Bill be amended to define the term 'concerns' national security.

Recommendation 36

6.156 The Committee recommends that the Bill be amended to define the term 'made available' for the purpose of the espionage offences.

Recommendation 37

6.158 The Committee recommends that the Bill be amended to introduce a prior publication defence for the proposed espionage offences. The defence should be appropriately drafted to ensure the effectiveness of the provisions whilst protecting freedom of expression and the implied constitutional right to freedom of political communication.

The Bill should further be amended to require that, prior to instituting proceedings to commit a person to trial for an espionage offence, the Attorney-General must consider whether the conduct might be authorised in any of the defences outlined in Division 91.

Recommendation 38

6.161 The Committee recommends that the Attorney-General's proposed amendments to narrow the scope of the offence in proposed section 91.3 of the Bill be implemented. This includes requiring that the person dealt with the information for the 'primary purpose' of making it available to a foreign principal, limiting the offence to information or articles that have a security classification, and removing strict liability from the offence.

Recommendation 39

6.163 The Committee recommends that the Explanatory Memorandum be amended to clarify the intended scope of the proposed defence in Division 91 for dealings 'in accordance with a law of the Commonwealth'. The Explanatory Memorandum should provide examples of situations in which conduct would be excused by the specific defence, but not the general defence of lawful authority available under section 10.5 of the *Criminal Code*.

Recommendation 40

6.165 The Committee recommends that the Bill be amended to limit the aggravating factor at subparagraph 91.6(1)(b)(v), in relation to the proposed espionage offences, to persons holding an Australian Government security clearance that allows the person to access information with a classification of SECRET or above.

Recommendation 41

6.168 The Committee recommends that the Explanatory Memorandum be amended so that the Statement of Compatibility with Human Rights explicitly addresses the limitation to the right to freedom of expression imposed by the espionage offences.

Recommendation 42

7.71 The Committee recommends that the Bill be amended to explicitly provide that the term 'support' refers to 'material support', and that the Explanatory

Memorandum provide examples of conduct that will not constitute material support, for example, news reporting, editorial or opinion writing and humanitarian assistance.

Recommendation 43

7.107 The Committee recommends that the Explanatory Memorandum be amended to clarify whether the offence is intended to capture the theft of trade secrets by hacking or other online vectors.

Recommendation 44

8.57 Consistent with the other sabotage offences in the Bill, the Committee recommends that proposed sections 82.7 and 82.8 (introducing vulnerability with intention, or recklessness, as to national security) be amended to remove the following elements:

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

Recommendation 45

8.60 The Committee recommends that the defence at proposed section 82.10, in relation to the Bill's sabotage offences, be broadened to include conduct engaged in on behalf of a private owner or operator of infrastructure, in addition to public officials.

Recommendation 46

9.99 The Committee recommends that the Bill be amended to define the term 'advocating' for the purpose of proposed section 83.1 (advocating mutiny), consistent with other existing offences in the *Criminal Code*.

Recommendation 47

9.103 The Committee recommends that the Bill be amended to provide that the 'good faith' defence at section 80.3 of the *Criminal Code* is available for the offence of advocating mutiny.

Recommendation 48

9.105 The Committee recommends that proposed section 83.5(4) 'Consent of Attorney-General required for prosecutions' be amended so that, for an offence against section 83.1 (advocating mutiny), the Attorney-General must consider whether conduct might be authorised in a way mentioned in section 80.3.

Recommendation 49

9.111 The Committee recommends that proposed section 83.3 (military style training involving foreign government) be amended to provide a defence against prosecution for those engaged in humanitarian work, including compliance training on the laws of armed conflict.

Recommendation 50

9.114 The Committee recommends that the Government reduce the penalty for the offence of 'interference with political rights and duties' at proposed section 83.4 from 10 years' imprisonment.

Recommendation 51

9.115 The Committee recommends that the Explanatory Memorandum be amended to clarify that nothing in the Bill affects the Parliament's powers in relation to contempt.

Recommendation 52

10.39 The Committee recommends that the Explanatory Memorandum be amended so that the Statement of Compatibility with Human Rights explicitly addresses the necessity, reasonableness, and proportionality of the expansion of telecommunications interceptions powers to all of the offences specified in Schedule 4 of the Bill.

Recommendation 53

10.62 The Committee recommends that Schedule 1, item 29 of the Bill be amended such that section 35A of the *Australia Citizenship Act 2007* applies to the foreign interference offences in the Bill, and does not apply to

- proposed section 82.9 (preparing for or planning sabotage offence),

- proposed section 83.4 (interference with political rights and duties), or
- proposed Part 5.6 – Secrecy of information.

Recommendation 54

10.74 The Committee recommends that the Bill be amended such that the phrase 'national security offence' in the *Australian Citizenship Act 2007* is limited to those offences which contain a clear nexus to national security.

Recommendation 55

10.75 The Committee recommends that the Explanatory Memorandum be amended so that the Statement of Compatibility with Human Rights explicitly addresses the interaction between the proposed consequential amendments to citizenship application provisions, and Australia's international obligations regarding stateless persons.

Recommendation 56

10.103 The Committee recommends that the Bill be amended to provide that section 15AA(1) of the *Crimes Act 1914* applies to an offence against proposed Division 80, Division 91, and Division 92 of the *Criminal Code* only if:

- the death of a person is alleged to have been caused by conduct that is a physical element of the offence, or
- conduct that is a physical element of the offence carried a substantial risk of causing the death of a person.

Recommendation 57

10.113 The Committee recommends that the Explanatory Memorandum for the Bill be amended to clarify the scope and application of section 93.2 of the *Criminal Code*.

Recommendation 58

10.125 The Committee recommends that the Bill be amended to provide that section 19AG of the *Crimes Act 1914*, relating to minimum non-parole

periods for certain offences, applies to an espionage offence against section 91.1(1) or 91.2(1), rather than all espionage offences in Division 91.

Recommendation 59

11.3 The Committee recommends that, after a period of three years, the Independent National Security Legislation Monitor be required to conduct a review of Division 82 (sabotage), Part 5.2 (espionage, foreign interference, theft of trade secrets), and Part 5.6 (secrecy) of the *Criminal Code*.

A copy of the report on the independent review should be provided to the Attorney-General, who should be required to provide it to the Committee. Any amendments proposed to be made to the laws as a result of the review should be referred to the Committee for inquiry.

Recommendation 60

11.5 The Committee recommends that the Attorney-General's Department review the Bill and Explanatory Memorandum in detail with a view to making amendments to correct any drafting errors prior to the conclusion of debate in the Parliament.

1. Current environment

1.1 The National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 (the Bill) and the Foreign Influence Transparency Scheme Bill 2017 (the Foreign Influence Transparency Scheme Bill) were introduced to the House of Representatives on 7 December 2017 by the Prime Minister, the Hon. Malcom Turnbull MP.

1.2 In his second reading speech, the Prime Minister advised the Parliament that both bills are 'designed to reinforce the strengths of our open democratic systems while shoring up its vulnerabilities'.[1] Currently, he declared, our agencies 'lack the legislative tools they [need] to act [and] … our system as a whole has not grasped the nature and magnitude of the threat'.[2]

1.3 In regards to the scale of threat, the Prime Minister quoted the Director-General of Security, Australian Security Intelligence Organisation (ASIO), who stated that the threat from espionage and foreign interference in Australia is 'unprecedented'.[3]

The current environment

1.4 ASIO advised the Committee that espionage and foreign interference activity against Australian interests is 'occurring at an unprecedented scale'. More specifically, ASIO advised:

---

1 The Hon. Malcolm Turnbull MP, Prime Minister, *House of Representatives Hansard*, 7 December 2017, p. 13147.

2 The Hon. Malcolm Turnbull MP, Prime Minister, *House of Representatives Hansard*, 7 December 2017, p. 13147.

3 The Hon. Malcolm Turnbull MP, Prime Minister, *House of Representatives Hansard*, 7 December 2017, p. 13145.

> This isn't something that we think might happen or could happen; it is happening now against Australian interests in Australia and Australian interests abroad. … Foreign actors from a range of countries seek access to privileged and/or classified information on Australia's alliances and partnerships, our position on international diplomatic, economic and military issues, our energy and mineral resources and our innovations in science and technology.[4]

1.5 The Director-General of Security, Mr Duncan Lewis, explained that in the current environment there is

> a more diverse range of hostile foreign intelligence services working against us than we've had in the past. … Many of these hostile foreign intelligence services have significantly increased the resources that are dedicated to foreign intelligence collection, and they have also greatly improved the spectrum and sophistication of their activities.[5]

1.6 In evidence to other inquiries of this Committee, ASIO has described the threat from espionage and foreign interference as 'extensive, unrelenting and increasingly sophisticated'.[6] During this inquiry, ASIO stated that though the harm from such activities may not be immediately apparent or overt, the consequences are far-reaching and serious. Such consequences include:

- undermining Australia's national security and sovereignty,
- damaging Australia's international reputation and relationships,
- degrading Australia's diplomatic and trade relations,
- inflicting substantial economic damage, and
- compromising nationally vital assets and critical infrastructure.[7]

---

4 Mr Peter Vickery, Deputy Director-General, Counter-Espionage and Interference and Capabilities, Australian Security Intelligence Organisation, *Committee Hansard*, Canberra, 31 January 2018, p. 18.

5 Mr Duncan Lewis, Director-General of Security, Australian Security Intelligence Organisation, *Committee Hansard*, Melbourne, 16 March 2018, p. 33.

6 Australian Security Intelligence Organisation, *Submission to Review of Administration and Expenditure No. 16 (2016-2017)*, Submission 5, p. 4.

7 Mr Peter Vickery, Deputy Director-General, Counter-Espionage and Interference and Capabilities, Australian Security Intelligence Organisation, *Committee Hansard*, Canberra, 31 January 2018, p. 18.

1.7 In addition to traditional espionage efforts to penetrate Australian governments, ASIO has outlined that foreign intelligence services are clandestinely targeting a range of other Australian interests, including our intellectual property, science and technology, and commercially sensitive information.[8]

1.8 Foreign intelligence services are increasingly using a wider range of techniques or 'vectors' to obtain intelligence and clandestinely interfere in Australia's affairs.[9] ASIO advised that the contemporary environment is unlike that of previous decades. The situation now is that Australia's adversaries are 'much more blurred', and Australia faces a raft of different countries that are seeking to conduct interference and exert influence in Australia.[10]

1.9 The Director-General of Security explained that in the 'information age', espionage activity in Australia is not limited to its 'classical form' where a foreign spy recruits an official for access to classified information. As a result of the features of globalisation, which has seen 'unimagined movement of money, … people [and] … information', espionage now includes 'more complex cyberintrusion that's conducted typically from overseas to enable the theft of sensitive technologies'. Such intrusion is 'comparatively cheap, … instantaneous and, most importantly, it's very difficult to detect and to attribute'.[11]

1.10 ASIO confirmed that it operates a threat level system in relation to foreign interference and espionage to measure the scale of the threat. However, unlike terrorism, that system is not an over-arching threat level system but rather operates on a country-by-country basis. For some countries, ASIO

---

8 Australian Security Intelligence Organisation, *Submission to Review of Administration and Expenditure No. 16 (2016-2017)*, Submission 5, p. 4.

9 Australian Security Intelligence Organisation, *Submission to Review of Administration and Expenditure No. 16 (2016-2017)*, Submission 5, p. 4; see also Mr Duncan Lewis, Director-General of Security, Australian Security Intelligence Organisation, *Committee Hansard*, Melbourne, 16 March 2018, pp. 33-34.

10 Mr Peter Vickery, Deputy Director-General, Counter-Espionage and Interference and Capabilities, Australian Security Intelligence Organisation, *Committee Hansard*, Canberra, 31 January 2018, p. 20.

11 Mr Duncan Lewis, Director-General of Security, Australian Security Intelligence Organisation, *Committee Hansard*, Melbourne, 16 March 2018, p. 33.

described the threat as 'extreme', indicating that foreign interference and espionage activities are occurring within Australia.[12]

1.11 These activities include targeting and attempting to recruit officials and persons of influence.[13] ASIO described the range of situations where this targeting and recruitment is occurring:

> These [officials] have undertaken activities in conscious collaboration with foreign intelligence officers in order to advance the national security interests of those foreign countries by seeking access to and obtaining privileged information and classified information in relation to Australia's views on a whole raft of issues. … They do this on many occasions for money, so there's a transactional relationship where a person is cultivated and recruited and, in return for money and finance, they provide privileged information which then goes back to that particular foreign intelligence service and is then used as part of, I suppose, that particular service's overall assessment of Australia's capabilities, vulnerabilities and weaknesses so that they can target the country—they can target politicians, business officials or intelligence officers—to get an advantage for them to our detriment.[14]

1.12 In comparison to espionage, the Director-General of Security described foreign interference as 'a far broader field of activity' that

> grows with the imagination and ambition of foreign powers, ranging from a foreign power using local Australians to observe and harass its diaspora community here in our country through to the recruitment and co-opting of influential and powerful Australian voices to lobby our decision-makers.
>
> … When looking at events such as the reported [attempted] assassination in the United Kingdom a week or two ago, which the Prime Minister has rightly

---

12 Mr Peter Vickery, Deputy Director-General, Counter-Espionage and Interference and Capabilities, Australian Security Intelligence Organisation, *Committee Hansard*, Canberra, 31 January 2018, p. 20.

13 Mr Peter Vickery, Deputy Director-General, Counter-Espionage and Interference and Capabilities, Australian Security Intelligence Organisation, *Committee Hansard*, Canberra, 31 January 2018, p. 21.

14 Mr Peter Vickery, Deputy Director-General, Counter-Espionage and Interference and Capabilities, Australian Security Intelligence Organisation, *Committee Hansard*, Canberra, 31 January 2018, p. 21.

> described as a heinous attack, we should not consider ourselves immune from such extreme acts.[15]

1.13 Beyond foreign interference and espionage, ASIO stated there has been a greater focus on *covert influence* operations, in addition to the traditional methods of human-enabled collection, technical collection and exploitation of the internet and information technology.[16] ASIO expanded on the extent of covert influence operations in its 2016-17 Annual Report:

> We identified foreign powers 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. Ethnic and religious communities in Australia were also the subject of covert influence operations designed to diminish their criticism of foreign governments.[17]

1.14 Such activities are undertaken covertly to obscure the role of foreign governments. ASIO advised that covert influence activities represent 'a threat to our sovereignty, the integrity of our national institutions and the exercise of our citizens' rights'.[18]

1.15 The extent of espionage, foreign interference and covert influence being undertaken in Australia was discussed in numerous submissions to this inquiry.[19] A number of submissions to the Committee's inquiry into the Foreign Influence Transparency Scheme Bill also referenced covert and clandestine activities targeting Australia's national interests.[20]

---

15 Mr Duncan Lewis, Director-General of Security, Australian Security Intelligence Organisation, *Committee Hansard*, Melbourne, 16 March 2018, pp. 33-34.

16 Australian Security Intelligence Organisation, *Submission to Review of Administration and Expenditure No. 16 (2016-2017)*, Submission 5, p. 4.

17 Australian Security Intelligence Organisation, *Annual Report 2016-17*, pp. 4-5.

18 Australian Security Intelligence Organisation, *Annual Report 2016-17*, pp. 4-5.

19 Mr Peter Jennings, *Submission 15*; Professor Clive Hamilton and Mr Alex Joske, *Submission 20*; Revd Dr Mark Durie, *Submission 22*; Ms Linda Jackobson, *Submission 28*; The Federation for a Democratic China, *Submission 32*; Professor Rory Medcalf, *Submission 33*; Chinese Community Council of Australia, *Submission 37*.

20 Epoch Times, Submission 23; Falun Dafa Association of Australia, *Submission 24*; Australian Values Alliance, *Submission 25*; John Fitzgerald, *Submission 26*; Dr Anne Marie Brady, *Submission 28*; Alexander Nilsen, *Submission 30*; Linda Jakobson, *Submission 39*; Chinese Community Council of Australia, *Submission 46*; The Federation of Chinese Associations (Victoria), *Submission 53*; Professor Rory Medcalf, *Submission 64*.

Government response to the threat

1.16 In his second reading speech the Prime Minister referred to a classified report, prepared by the Department of the Prime Minister and Cabinet, which contained advice from ASIO of 'significant investigative breakthroughs and delivered a series of very grave warnings'.[21] In response to these discoveries, collectively this Bill and the Foreign Influence Transparency Scheme Bill are intended to 'counter the threat of foreign states exerting improper influence over our system of government and our political landscape'.[22]

1.17 The two Bills form part of the Government's Counter Foreign Interference Strategy. The Strategy has four pillars: sunlight, enforcement, deterrence and capability:

> [O]ur rejection of covert, coercive or corrupting behaviour leads naturally to a counter-foreign-interference strategy that is built upon the four pillars of sunlight, enforcement, deterrence and capability.
>
> It means that if you use inducements or threats to manipulate a political process or public debate then we will unleash the full force of powerful new laws and defend our values and democratic institutions.
>
> And it means that foreign actors who would do us harm are now on notice: we will not tolerate covert, coercive or corrupting behaviour in our country.[23]

1.18 The Espionage and Foreign Interference Bill is directed at the second and third of those pillars: 'enforcement' and 'deterrence'. The Prime Minister noted that the Bill will work in tandem with the Foreign Influence Transparency Scheme, which is directed at the first of pillar, 'sunlight'.

1.19 At a public hearing, the Director-General of Security advised the Committee that ASIO 'strongly supports' the Espionage and Foreign Interference Bill, and 'supports' measures to increase the transparency surrounding foreign influence in Australia. The Director-General stated that the reforms will

---

21 The Hon. Malcolm Turnbull MP, Prime Minister, *House of Representatives Hansard*, 7 December 2017, p. 13147.

22 The Hon. Malcolm Turnbull MP, Prime Minister, *House of Representatives Hansard*, 7 December 2017, p. 13145.

23 The Hon Malcolm Turnbull MP, Prime Minister, *House of Representatives Hansard*, 7 December 2017, p. 13145.

provide 'integral and urgently required tools to help combat the unprecedented scale of espionage and foreign interference activities currently being conducted against us'.[24]

1.20 Significantly, the Attorney-General's Department (the Department) sought to contrast 'foreign interference'—to which the Bill is directed—and 'foreign influence'—to which the Foreign Influence Transparency Scheme is addressed—as distinct concepts.[25] ASIO however advised the Committee that the two terms are 'interrelated',[26] and 'intertwined to the point where you can have one leading to the other'.[27]

1.21 This report presents the Committee's review of the Espionage and Foreign Interference Bill. The Committee's review of the Foreign Influence Transparency Scheme Bill is provided in a separate report.

1.22 The Director-General of Security, in strongly supporting the Espionage and Foreign Interference Bill,[28] advised the Committee that, 'the current criminal offences are inadequate to deal with the foreign intelligence threat that we now face' and described existing offences as 'outdated and deficient' and 'inadequate or unworkable'.[29] As a result, ASIO assessed that the 'net effect is that our nation's freedom of decision-making and core interests are not adequately protected by the rule of law'.[30]

1.23 The Director-General also advised the Committee of the anticipated deterrent effect of the Espionage and Foreign Interference Bill, stating:

---

24 Mr Duncan Lewis, Director-General of Security, Australian Security Intelligence Organisation, *Committee Hansard*, Melbourne, 16 March 2018, p. 33.

25 Ms Anna Harmer, First Assistant Secretary, Security and Criminal Law Division, Attorney-General's Department, *Committee Hansard*, Canberra, 31 January 2018, p. 16.

26 Mr Duncan Lewis, Director-General of Security, Australian Security Intelligence Organisation, *Committee Hansard*, Melbourne, 16 March 2018, p. 38.

27 Mr Peter Vickery, Deputy Director-General, Counter-Espionage and Interference and Capabilities, Australian Security Intelligence Organisation, *Committee Hansard*, Melbourne, 16 March 2018, p. 38.

28 Mr Duncan Lewis, Director-General Security, Australian Security Intelligence Organisation, *Committee Hansard*, Melbourne, 16 March 2018, p. 33.

29 Mr Duncan Lewis, Director-General Security, Australian Security Intelligence Organisation, *Committee Hansard*, Melbourne, 16 March 2018, p. 34.

30 Mr Duncan Lewis, Director-General Security, Australian Security Intelligence Organisation, *Committee Hansard*, Melbourne, 16 March 2018, p. 34.

> There's a pressing requirement to deter hostile foreign spies who are conducting espionage and foreign interference against Australian interests as we sit here today. The proposed laws would, in my view, make Australia a much harder target for foreign intelligence services. It would be demonstrably more difficult to operate here. … Facing no realistic prospect of criminal investigation and prosecution for their activities against us, our foreign adversaries are currently shielded from the significant disincentive of public exposure and punishment, and they are taking advantage of this gap. … Criminal prosecutions for espionage, foreign interference, secrecy, sabotage and economic espionage offences that are tested in our courts and reported in our media will send a very powerful message to those orchestrating such activity against us.[31]

1.24 Many participants in the inquiry supported strengthened measures to deal with the threat posed by increased espionage and foreign interference activities in Australia.[32] Submitters also called for caution to ensure that innocuous or beneficial conduct is not caught up in the proposed new offences,[33] and that sections of the Australian community are not adversely affected.[34]

---

31 Mr Duncan Lewis, Director-General Security, Australian Security Intelligence Organisation, *Committee Hansard*, Melbourne, 16 March 2018, p. 34.

32 Peter Jennings, *Submission 15*; Clive Hamilton and Alex Joske, *Submission 20*; Revd Dr Mark Durie, *Submission 22*, Alexander Nilsen, *Submission 24*; Federation for a Democratic China, *Submission 32*; Professor Rory Medcalf, *Submission 33*; Wal Walker, *Submission 42*; Scholars of China, the Chinese diaspora, China-Australia relations and Australia's relations with Asia, *Submission 50*.

33 Tony Kevin, *Submission 1*; Benji Wakely, *Submission 2*; E. Anne Lanham, *Submission 3*; Lucy Strange, *Submission 4*; Law Council of Australia, *Submission 5*; Australian Lawyers for Human Rights, *Submission 7*; Joint media organisations, *Submission 9*; Human Rights Watch, *Submission 10*; Human Rights Law Centre, *Submission 11*; Australian Lawyers Alliance, *Submission 12*; Valarie Heath, *Submission 14*; Australian Human Rights Commission, *Submission 17*; Dr Lawrence McNamara, University of York, *Submission 19*; Centre for Media Transition, University of Technology, Sydney, *Submission 23*; Chris Morris, *Submission 25*; *Submission 26* (name withheld); Australian Conservation Foundation, *Submission 29*; United Nations Special Rapporteurs, *Submission 30*; Joint councils for civil liberties, *Submission 31*; Digital Rights Watch, *Submission 34*; Nyman Gibson Miralis, *Submission 35*; WWF-Australia, *Submission 36*; Chinese Community Council of Australia, *Submission 37*; GetUp, *Submission 38*; 350.org, *Submission 39*; Dr Luke Beck, *Submission 41*; Greenpeace Australia Pacific, *Submission 43*; *Submissions 45 to 49* (form letters).

34 Linda Jakobson, *Submission 28*; Chinese Community Council of Australia, *Submission 37*; Joint submission from scholars of China and the Chinese diaspora, *Submission 44*.

Committee comment

1.25 During its inquiry, the Committee has received compelling evidence that Australia is facing an unprecedented threat from espionage and foreign interference. The Committee has also received evidence that current laws are not adequate to deal with this threat. Unchecked, espionage has the potential to significantly reduce Australia's long-term security, and foreign interference could undermine our democracy and threaten the rights and freedoms of our people.

1.26 The Committee therefore accepts that there is a pressing need to strengthen and modernise current espionage and foreign interference laws.

1.27 The Committee understands that prosecution for criminal offences is not the only means available to authorities to deal with espionage and foreign interference activity. It is, however, important to have criminal laws that are sufficiently robust to deter the full range of activity that foreign actors may seek to employ.

1.28 The Committee supports the intent of the Bill to achieve these goals and, subject to the other recommendations in this report, the Committee supports its passage through the Parliament.

Recommendation 1

1.29 The Committee recommends that, following implementation of the recommendations in this report, the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 be passed.

1.30 Having accepted that it is necessary to strengthen espionage and foreign interference laws in response to the current threat environment, the Committee has considered the common principles to be applied to its analysis of the laws directed at meeting this threat. In summary, the Committee considers that laws need to be effective at achieving their stated aims, at the same time as minimising any limitations on human rights.

1.31 To be effective, the laws need to be workable from the perspective of law enforcement and prosecutors—that is, they must be enforceable.

1.32 In relation to minimising limitations on human rights, the Australian Human Rights Commission has previously advised the Committee that it is permissible for a legislative measure to limit human rights where the

measure is expressed in clear and unambiguous terms, is directed to a legitimate aim, is necessary to achieve that aim, and is proportionate.[35]

1.33 Taking these considerations together, and having accepted the legitimacy of the aims of the Bill, the Committee has sought to ensure through its review that each of the measures in the Bill is:

- clear and unambiguous in its terms,
- proportional and appropriately targeted to the threat, and
- enforceable.

35 Australian Human Rights Commission, *Submission 3.1 to the Review of the 'declared area' provisions*, p. 5.

2. The Bill and its referral

The Bill and its referral

2.1 On 7 December 2017, the Prime Minister, the Hon. Malcolm Turnbull MP, introduced a package of national security bills into the House of Representatives. The bills included:

- Foreign Influence Transparency Scheme Bill 2017;
- National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017; and
- Home Affairs and Integrity Agencies Legislation Amendment Bill 2017.

2.2 On 8 December 2017, the Prime Minister referred the bills to the Committee, requesting that the Committee, so far as possible, conduct its inquiry in public.

2.3 This report is the Committee's review of the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017 (the Bill).

Objectives of the Bill

2.4 The Prime Minister's referral letter noted that, following the Prime Minister's direction on 12 May 2017, the Attorney-General had conducted a 'comprehensive review of Australia's espionage and foreign interference laws'. The review considered:

- the adequacy and effectiveness of existing espionage and treason offences under the *Criminal Code Act 1995* and the official secrets offences under the *Crimes Act 1914*,
- 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 complementary provisions that would strengthen agencies' ability to investigate and prosecute acts of espionage and foreign interference.

2.5 The letter summarised the outcomes of the review as follows:

> The legislative package implements the outcomes of the Attorney-General's review. Australia's existing criminal laws are not fully effective in deterring and countering pervasive foreign interference activities directed against our interests. In particular, existing criminal laws relating to espionage, secrecy, sabotage and treason needed to be updated, and new foreign interference and theft of trade secrets offences enacted, to ensure Australia is not a permissive operating environment for malicious foreign actors.
>
> Australian law should also require transparency around activities undertaken in Australia on behalf of foreign principals where the activities are intended to influence political or government processes.

2.6 The Bill repeals existing criminal offences and introduces a range of new offences into the *Criminal Code* in relation to espionage, foreign interference, sabotage of public infrastructure, and secrecy of Commonwealth information. The Bill also amends a range of existing offences, including those in relation to treason, treachery, and other threats to security.

2.7 According to its Explanatory Memorandum, the objective of the Bill is to

> modernise and strengthen Australia's espionage, foreign interference, secrecy and related laws to ensure the protection of Australia's security and Australian interests.[1]

2.8 The Explanatory Memorandum states that existing laws do not adequately counter these activities. Rather, a lack of serious criminal penalties and law enforcement powers in the current laws is said to have resulted in a 'permissive operating environment for malicious foreign actors'.[2] The Explanatory Memorandum states:

> Foreign actors are currently seeking to harm Australian interests on an unprecedented scale, posing a grave threat to Australia's sovereignty,

---

1 Explanatory Memorandum, p. 11.

2 Explanatory Memorandum, p. 11.

> prosperity and national security. This threat is a substantial concern for the Australian Government. If left unchecked, espionage and foreign interference activities may diminish public confidence in the integrity of political and government institutions, compromise Australia's military capabilities and alliance relationships, and undercut economic and business interests within Australia and overseas.[3]

2.9 The objectives of the specific measures in the Bill are discussed in the context of each offence later in this report.

Conduct of the inquiry

2.10 After receiving the Prime Minister's referral, the Committee initially agreed to complete its inquiry and report to the Parliament by 20 February 2018, and later extended this date to 23 March 2018. Following the receipt of proposed Government amendments to the Bill on 5 March 2018 (discussed later in this report), the Committee further extended its reporting date.

2.11 The Chair of the Committee, Mr Andrew Hastie MP, announced the inquiry by media release on 15 December 2017 and invited submissions from interested members of the public.

2.12 The Committee received 51 submissions and 20 supplementary submissions. 2543 form letters were also received to the inquiry. A list of submissions received by the Committee is at Appendix A.

2.13 The Committee held five public hearings and one private hearing in Canberra on 30 and 31 January, 15 and 16 February, and 16 March 2018. Details of the hearings are included at Appendix B. The Committee also received two classified briefings.

2.14 Copies of submissions and the transcript from the public hearing can be accessed on the Committee's website at www.aph.gov.au/pjcis. Links to the Bill and Explanatory Memorandum are also available on the Committee's website.

Timeframe for the inquiry

2.15 In referring the Bill, the Prime Minister asked that the Committee present its report by 15 February 2018.

---

[3] Explanatory Memorandum, p. 11.

2.16 A number of submitters raised concerns regarding the timeframe for the inquiry.

2.17 As noted in previous reports, the Committee considers it performs a vital role in scrutinising national security legislation prior to its consideration by the Parliament. Over the last five years the Committee has examined every national security bill and has made a significant number of recommendations—these recommendations have gone to strengthening the integrity, operation, clarity and oversight of national security measures. The Government has agreed to all the Committee's recommendations made on various bills.

2.18 These significant and unprecedented new measures in relation to foreign influence and interference in Australia require careful consideration and the Committee is pleased to undertake this inquiry. In the current climate, Australia must seek to protect the integrity of its national institutions against both covert interference and obscured influence.

2.19 However, to perform these functions effectively, time is needed for public consultations. This enables the Committee to interrogate a bill, and ensure the integrity and proportionality of the proposed measures, clarity and effectiveness in their application and operation, and an adequacy of safeguards. In this instance, the Committee was requested to inquire into and report on these complex issues in ten weeks which included the Christmas/New Year holiday period. The Committee reiterates previous requests that, as far as possible when considering the need for future national security legislation, sufficient time be provided for the Committee to undertake a comprehensive inquiry. This is particularly necessary where no prior public consultation on a Bill has been conducted by the relevant departments.

Report structure

2.20 This report consists of 11 chapters:

- Chapter 1 discusses the current threat environment that provides the context for the Committee's inquiry,
- the remainder of Chapter 2 summarises the contents of the Bill and its structure,
- Chapter 3 discusses certain issues that were raised during the Committee's inquiry that concern more than one of the Bill's components,

- Chapter 4 discusses the rationale for and breadth of conduct captured by the new secrecy offences proposed in the Bill,
- Chapter 5 discusses the defences available and other matters relating to the new secrecy offences proposed the Bill,
- Chapter 6 discusses the new espionage offense proposed in the Bill,
- Chapter 7 discusses the new foreign interference offences and the theft of trade secrets offence proposed in the Bill,
- Chapter 8 discusses the new sabotage offences proposed in the Bill,
- Chapter 9 discusses the revised offences for treason, treachery and other threats to security proposed in the Bill,
- Chapter 10 discusses Schedules 3 to 5 of the Bill, and a range of consequential amendments contained in Schedules 1 and 2, and
- Chapter 11 contains the Committee's concluding comments.

Outline of the Bill

2.21 The Bill comprises five schedules, mostly affecting the *Criminal Code Act 1995*. The Bill also proposes a range of consequential and other amendments to the following Acts:

- *Aboriginal and Torres Strait Islander Act 2005*
- *Agricultural and Veterinary Chemicals (Administration) Act 1992*
- *Archives Act 1983*
- *Australian Citizenship Act 2007*
- *Australian Crime Commission Act 2002*
- *Australian Federal Police Act 1979*
- *Commonwealth Electoral Act 1918*
- *Chemical Weapons (Prohibition) Act 1994*
- *Comprehensive Nuclear-Test-Ban Treaty Act 1998*
- *Crimes Act 1914*
- *Defence Home Ownership Assistance Scheme Act 2008*
- *Freedom of Information Act 1982*
- *Foreign Evidence Act 1994*
- *Law Enforcement Integrity Commissioner Act 2006*
- *Liquid Fuel Emergency Act 1984*
- *Migration Act 1958*
- *National Greenhouse and Energy Reporting Act 2007*
- *Native Title Act 1993*
- *Offshore Minerals Act 1994*
- *Ombudsman Act 1976*

- *Parliamentary Service Act 1999*
- *Public Service Act 1999*
- *Renewable Energy (Electricity) Act 2000*
- *Surveillance Devices Act 2004*
- *Textile, Clothing and Footwear Investment and Innovation Programs Act 1999*
- *Telecommunications (Interception and Access) Act 1979*
- *Foreign Influence Transparency Scheme Act 2017*

Box 2.1 Summary of proposed amendments

- Offences
  - replaces and broadens existing espionage and sabotage offences
  - introduces new categories of offences, including foreign interference and theft of trade secrets
  - revises other offences against the state, including treason and treachery
  - replaces and broadens existing secrecy offences
  - creates a new aggravated offence for giving false or misleading information in connection with a security clearance
- Investigations and proceedings
  - enables law enforcement agencies to use telecommunications interception powers to investigate new offences
  - broadens the range of proceedings which can be held in camera
- Consequential amendments.

Schedule 1- Treason, espionage, foreign interference and related offences

2.22 Schedule 1 amends and introduces a range of new or modernised offences against the security of the Commonwealth into Parts 5.1 and 5.2 of the *Criminal Code*.

Treason (Item 4, clause 80.1AA)

2.23 The Bill amends the existing offence of 'Treason—materially assisting enemies etc' in section 80.1AA of the *Criminal Code* to align with modern terminology related to armed conflict. Treason offences continue to carry a maximum term of imprisonment for life.

Treachery (Item 4, clause 80.1AC)

2.24 The Bill replaces the existing treachery offence in Part II of the *Crimes Act 1914* with a new offence in Part 5.1, Division 80 of the *Criminal Code*.

2.25 The current treachery offence criminalises conduct against both Australia and other countries, including attempts to overthrow the government, levy war against or instigate an invasion into a proclaimed country. The amendments proposed in Schedule 1 will limit the treachery offence to conduct engaged in with the intent of overthrowing the Commonwealth Government, the Australian Constitution, or the government of an Australian state or territory. The amendments also extend the offence to conduct engaged in with the intent of overthrowing the 'lawful authority' of the Commonwealth Government. The offence continues to carry a maximum penalty of imprisonment for life.

Sabotage (Item 8)

2.26 The Bill replaces the current sabotage offence in Part II of the *Crimes Act 1914* with seven new offences in Part 5.1, Division 82 of the *Criminal Code*. While the existing offences are limited to defence property, the proposed new sabotage offences are premised on damage caused or vulnerabilities introduced to 'public infrastructure'. The term 'public infrastructure' is broadly defined to cover a range of public and private interests. The proposed offences relate to conduct involving:

- sabotage of public infrastructure, including sabotage of public infrastructure involving a foreign principal, where the person intends to, or is reckless as to whether the sabotage would prejudice Australia's national security, or advantage another country's national security,
- introducing vulnerability to public infrastructure, where the person intends or is reckless as to whether the conduct will:
  - prejudice Australia's national security, or
  - harm or prejudice Australia's economic interests, or
  - disrupt state or Federal Government functions, or
  - damage public infrastructure,
- preparing or planning sabotage or the introduction of vulnerability to public infrastructure.

2.27 The proposed amendments will increase the maximum penalty for a sabotage offence from 15 years to 25 years. The maximum penalties for the

other offences introduced into this Division range from seven to 20 years imprisonment.

2.28 The Bill creates a defence against the Division for certain conduct by public officials, in addition to the general defences available in Part 2.3 of the *Criminal Code*.

2.29 The amendments require the Attorney-General to consent to a person being committed for trial for offences against this Division. The Bill proposes that, when deciding whether to provide this consent, the Attorney-General must consider whether the person's conduct might be authorised in a way mentioned in the defences outlined in the Division. The Attorney-General's consent is not required to arrest, charge or remand an accused person in custody or on bail.

Other threats to security (Item 8)

2.30 The Bill inserts new versions of other existing offences against the state into Part 5.1, Division 83 of the *Criminal Code*, including:

- advocating mutiny—renamed and with broader application than the 'inciting mutiny' offence in Part II of the *Crimes Act 1914*, and carrying a reduced maximum penalty,
- assisting prisoners of war to escape—which will carry a reduced maximum penalty compared to the existing offence in Part II of the *Crimes Act 1914*,
- military-style training involving a foreign government principal—renamed from the 'unlawful drilling' offence in Part II of the *Crimes Act 1914* and carrying an increased maximum penalty, and
- interference with political rights and duties, renamed from the existing 'interfering with political liberty' offence in Part II of the *Crimes Act 1914* and carrying an increased maximum penalty.

2.31 The penalties for these offences will range from seven to 20 years imprisonment.

2.32 The amendments require the Attorney-General to consent to a person being committed for trial for these offences. This is not currently required. The Bill proposes that when deciding whether to consent to committing the accused person to trial for the offence of 'military-style training involving foreign government principal' or 'interference with political rights and duties' the Attorney-General must consider whether the person's conduct might be

authorised in a way mentioned in the defences outlined in Division 83. The Attorney-General's consent is not required to arrest, charge or remand an accused person in custody or on bail.

Espionage and related offences (Item 17)

2.33 Schedule 1 will amend Part 5.2 (Division 91) of the *Criminal Code* to replace current espionage laws. The new offences deal with information or articles 'made available' to foreign principals. The Bill introduces a range of new offences relating to espionage, including:

- dealings with information intentionally or recklessly prejudicing Australia's national security (proposed sections 91.1 and 91.2),
- dealing with information that has a security classification or that 'concerns' Australia's national security (proposed section 91.3),
- aggravated espionage offences (proposed section 91.6),
- espionage on behalf of a foreign principal (proposed section 91.8)
- soliciting, procuring, or making it easier to commit an espionage offence (proposed section 91.11), and
- preparing for an espionage offence (proposed section 91.12).

2.34 The offences will be broader in scope than current espionage offences, capturing a range of information including classified information; information concerning Australia's 'national security'; and any other information made available to a foreign principal with intent or recklessness as to national security.

2.35 For the purposes of Part 5.2, and Division 82 of Part 5.1 of the *Criminal Code*, the amendments will introduce a definition of the 'national security' of Australia and other countries. The definition is similar to but broader in scope than the definition of Australia's 'security' provided in the *Australian Security Intelligence Organisation Act 1979*,[4] and will include a country's political, military or economic relations with other countries.

---

[4] Section 4 of the *Australian Security Intelligence Organisation Act 1979* provides: 'security means:

(a) the protection of, and of the people of, the Commonwealth and the several States and Territories from:

(i) espionage;

(ii) sabotage;

(iii) politically motivated violence;

(iv) promotion of communal violence;

2.36 The amended espionage offences will increase the maximum penalty for espionage offences from 25 years imprisonment to imprisonment for life. The penalties for other offences introduced into Part 5.2 range from maximum terms of 15 to 25 years imprisonment.

2.37 A range of defences against the proposed offences will be introduced, in addition to the general defences available in Part 2.3 of the *Criminal Code*.

2.38 Schedule 1 continues to require the Attorney-General to consent to a person being committed for trial for offences against Part 5.2. The Bill proposes that when deciding whether to consent to committing the accused person to trial the Attorney-General must consider whether the person's conduct might be authorised in a way mentioned in the various defences outlined in Part 5.2. The Attorney-General's consent is not required to arrest, charge or remand an accused person in custody or on bail.

Foreign interference and theft of trade secrets (Item 17)

2.39 Schedule 1 will insert nine new foreign interference offences into Part 5.2 (Division 92) of the *Criminal Code*, including:

- intentional or reckless foreign interference,
- preparing for a foreign interference offence, and
- recklessly or knowingly supporting, funding or being funded by a foreign intelligence agency.

2.40 The proposed offences are intended to target conduct that is described as 'falling short' of traditional espionage, treason and secrecy offences.[5] The new offences will capture conduct undertaken on behalf of, or in support of, a foreign principal; and which is covert, deceptive, menacing or undisclosed. 'Foreign principal' will be defined broadly to encompass a range of foreign

---

(v) attacks on Australia's defence system; or

(vi) acts of foreign interference;

whether directed from, or committed within, Australia or not; and

(aa) the protection of Australia's territorial and border integrity from serious threats; and

(b) the carrying out of Australia's responsibilities to any foreign country in relation to a matter mentioned in any of the subparagraphs of paragraph (a) or the matter mentioned in paragraph (aa).

5 Attorney-General's Department, *Submission 6*, p. 7.

actors: including public organisations, public enterprises, terrorist organisations and the local or regional governments of foreign countries.

2.41 A range of defences against the proposed offences will be introduced, in addition to the general defences available in Part 2.3 of the *Criminal Code*.

2.42 The Bill also inserts a new offence for theft of trade secrets involving a foreign government principal into Part 5.2 (Division 92A). The new division will make it an offence to dishonestly receive, obtain, take, copy or duplicate, sell, buy or disclose information that is a trade secret on behalf of a foreign government principal.

2.43 Schedule 1 continues to require the Attorney-General to consent to a person being committed for trial for offences against Part 5.2. The Bill proposes that when deciding whether to consent to committing the accused person to trial the Attorney-General must consider whether the person's conduct might be authorised in a way mentioned in the various defences outlined in Part 5.2. The Attorney-General's consent is not required to arrest, charge or remand an accused person in custody or on bail.

In Camera Proceedings (Item 19)

2.44 The amendments proposed in Schedule 1 will enable judicial officers to hold a broader range of proceedings relating to Part 5.2 of the *Criminal Code* in camera. Currently, section 93.2 of the *Criminal Code* enables judicial officers to order proceedings heard in federal courts, territory courts, or other courts exercising federal jurisdiction to be held in camera where it is in the 'interest of the security or defence of the Commonwealth'. The proposed amendments will change this threshold, to being in the interests of Australia's 'national security', which will be defined to include Australia's political, military or economic relations with other countries.

Destroying or damaging Commonwealth property (Item 22)

2.45 The offence of destroying or damaging Commonwealth property will be removed from Part II of the *Crimes Act 1914* and inserted into Part 7.2 of the *Criminal Code*, which deals with theft and other property offences. The penalty for this offence will not be changed, and remains as a maximum term of ten years of imprisonment.

Schedule 2 – Secrecy

2.46 Schedule 2 introduces a new Part 5.6 to the *Criminal Code* to replace the current secrecy provisions set out in Parts VI and VII of the *Crimes Act 1914*.

2.47 The proposed offences are broader in scope than current offences. The provisions capture the conduct of any person, and any type of information, so long as that information was originally made or obtained by a person by reason of that person being a Commonwealth officer or otherwise engaged to work for the Commonwealth.

2.48 The offences proposed in Schedule 2 will regulate conduct involving 'inherently harmful information' (proposed section 122.1); conduct involving any information which does, will or is likely to cause harm to Australia's interests (proposed section 122.2). The offences will capture:

- 'dealings', including intentionally receiving, obtaining, collecting, possessing, making a record of, copying, altering, concealing, communicating, publishing or making information available,
- removing information from its place of proper custody or holding such information outside a proper place of custody,
- failing to comply with a direction regarding the retention, use or disposal of such information, and
- aggravated offences for the above conduct (proposed section 122.3).

2.49 Schedule 2 will also replace the existing offence of unauthorised disclosure by a current or former Commonwealth officer in section 79 of the *Crimes Act 1914* with a similar offence in section 122.4 the *Criminal Code*.

Inherently harmful information

2.50 The offences proposed in section 122.1 create, in effect, a general prohibition on all 'dealings' with 'inherently harmful information' made or obtained by a Commonwealth officer or person otherwise engaged to work for the Commonwealth, by virtue of their position. 'Inherently harmful information' is defined in section 121.1 to include:

- security classified information,
- information made or obtained by a domestic or foreign intelligence agency,

- information relating to the operations, capabilities, technologies of, methods or sources used by domestic of foreign law enforcement agencies, or
- information compulsorily acquired by the Commonwealth from a person.

2.51 In contrast to the provisions in proposed section 122.2, the offences do not require the person dealing with the information to cause harm, or intend to cause harm to Australia's national security, or Australia's interests.

Conduct causing harm to Australia's interests

2.52 The offences in proposed section 122.2 criminalise dealings with any information made or obtained by a person by reason of that person being a Commonwealth officer or otherwise engaged to work for the Commonwealth, where the conduct causes, will cause or is likely to cause harm to Australia's interests. The phrase 'cause harm to Australia's interests' is defined in proposed section 121.1 to include interfering with or prejudicing:

- the prevention, detection, investigation, prosecution or punishment of Commonwealth criminal offences and civil penalty provisions,
- certain functions of the Australian Federal Police,
- Australia's international relations, meaning Australia's political, military and economic relations with foreign governments and international organisations,[6]
- the relations between the Commonwealth and a State or Territory; and
- the health or safety of the public or a section of the public.

Defences

2.53 The amendments include a range of defences to these offences. The defendant bears an evidential burden in relation to these defences, which means that the defendant must point to evidence that suggests a reasonable possibility that the defence is made out. If achieved, the prosecution must then refute the defence beyond reasonable doubt.

---

[6] Proposed section 121.1 adopts the definition of 'international relations' provided in the *National Security Information (Criminal and Civil Proceedings) Act 2004*, which provides: 'international relations means political, military and economic relations with foreign governments and international organisations'.

2.54 All persons dealing with 'inherently harmful information' will need to rely upon these provisions.

Penalties

2.55 The maximum sentence for a breach of the secrecy provisions will be increased from the current seven year maximum penalty, to a maximum penalty of 20 years imprisonment for aggravated offences. The penalties range between two and 20 years imprisonment.

Consent not required to initiate proceedings

2.56 The consent of the Attorney-General is not proposed to be required to institute proceedings against a person for any of the secrecy offences. This is in contrast to the current 'official secrets' offence contained in section 79 of the *Crimes Act 1914*.[7]

Schedule 3 – Aggravated offence for giving false or misleading information

2.57 Schedule 3 amends Division 137 of Part 7.4 of the *Criminal Code* to create a new aggravated offence for providing false or misleading information. The offence arises where a person gives false or misleading information or omits certain information in connection with an Australian Government security clearance. The underlying offence carries a maximum penalty of imprisonment for one year. The proposed aggravated offence will carry a maximum penalty of imprisonment for five years.

Schedule 4 - Telecommunications serious offences

2.58 Schedule 4 amends the definition of 'serious offence' in section 5D of the *Telecommunications (Interception and Access) Act 1979*. The proposed amendments will enable the Australian Federal Police, the Australian Commission for Law Enforcement Integrity and the Australian Criminal Intelligence Commission to apply to an issuing authority for a telecommunications interception warrant for the purpose of investigating the offences proposed in the Bill.

---

[7] *Crimes Act 1914*, section 85. Note: the existing offence 'Disclosure of information by Commonwealth officers' contained in section 70 of the *Crimes Act 1914* (largely replicated in proposed section 122.4 of the *Criminal Code*), does not currently require consent to proceed.

Schedule 5 - Foreign Influence Transparency Scheme

2.59 Schedule 5 of the Bill will amend the *Foreign Influence Transparency Scheme Act 2017* (FITS Bill), if and once the Foreign Influence Transparency Scheme Bill 2017 and the Electoral Legislation Amendment (Electoral Funding and Disclosure Reform) Bill 2017 have been passed by the Parliament. The amendments will:

- align the disclosure threshold for donor activity under the Foreign Influence Transparency Scheme with the disclosure threshold in the Commonwealth Electoral Act ($13 500),[8] and
- import the term 'political campaigners'[9] into the Foreign Influence Transparency Scheme so that:
  - lobbying a political campaigner could be a registrable activity, and
  - influencing processes in relation to a political campaigner could be a registrable activity.

[8] The Electoral Bill will amend the definition of 'disclosure threshold' in the *Commonwealth Electoral Act 1918* to be $13 500 (which will be subject to indexation).

[9] The term political campaigner will be a new definition inserted into the *Commonwealth Electoral Act 1918* to mean a person or entity that is registered as a political campaigner under section 287L (this will cover entities where the amount of political expenditure incurred by or with the authority of the person or entity during that or any one of the previous 3 financial years is $100 000 or more; or the amount of political expenditure incurred by or with the authority of the person or entity: during that financial year is $50 000 or more; and during the previous financial year was at least 50% of the person or entity's allowable amount).

3. General issues across the Bill

3.1 In addition to commenting on the individual components of the Bill (discussed in subsequent chapters), certain issues were raised in the Committee's inquiry that concern more than one of the Bill's components. These include:

- the scope of key definitions, including 'national security', 'foreign principal', 'foreign intelligence agency' and 'Australian Government security clearance',
- issues concerning the incorporation of 'security classifications' into some offences,
- the provision for evidentiary certificates to be issued by the Attorney-General in relation to whether information is security classified or concerns national security,
- the inclusion of preparatory offences in relation to sabotage, espionage and foreign interference offences,
- the inclusion of reckless elements in some offences,
- the Bill's approach to placing evidentiary burden on the defendant, and
- protections for the rights to freedom of expression and freedom of political communication.

Scope of key definitions

Definition of 'national security'

3.2 The Bill proposes to introduce the term 'national security', which the Bill relies upon to determine the scope of a number of provisions, including the

new espionage, sabotage and foreign interference offences.[1] Proposed subsection 90.4(1) of the *Criminal Code* defines national security of Australia or a foreign country as:

a. the defence of the country,

b. the protection of the country, the people of the country or any Part of it, from certain activities covered by subsection (2),

c. the protection of the integrity of the country's territory and borders from serious threats,

d. the carrying out of the country's responsibilities to any other country in relation to the matter mentioned in paragraph (c) or activities covered by subsection (2),

e. the country's political, military or economic relations with another country or other countries.

3.3 Subsection 90.4(2) outlines the activities referred to in paragraphs (b) and (d) above, namely:

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

3.4 The Explanatory Memorandum states that the purpose of the definition of 'national security' is

> to exhaustively cover the matters relevant to the security and defence of a country. The definition needs to cover matters relevant to Australia's national security as well as the national security of a foreign country.[2]

---

1 Refer to proposed Division 82 (sabotage), Division 91(espionage), Division 92 (foreign interference); and ss. 93.2 (in camera proceedings) and 93.3 (evidentiary certificates) of the *Criminal Code*.

2 Explanatory Memorandum, p. 103.

Breadth of definition

3.5 A number of participants in the inquiry expressed concern about the breadth of the definition.[3] For example, the Australian Lawyers Alliance (ALA) considered that elements of the definition would:

> expand national security beyond the traditional confines of the work of intelligence and security agencies to cover matters that are usually considered squarely within standard government. The ALA questions why the government is seeking to expand this concept so significantly, and is concerned that such an expansion could obscure damaging government practices, including illegal activities and corruption.[4]

3.6 Similarly, the Law Council of Australia argued:

> The breadth of the expression 'national security' extending to the country's political or economic relations with another country or countries may have a stifling effect on freedom of expression.[5]

3.7 GetUp considered that, due to the broad definition of national security, the offences in the Bill would 'impact upon GetUp's campaigning on issues such as the Trans-Pacific Partnership, refugees and climate change'.[6]

3.8 The Australian Lawyers for Human Rights also submitted that

> to include economic relations or interests as national security matters is unworkably vague and will have an unreasonably chilling impact on freedom of speech and discourse regarding matters of genuine public interest. This is inconsistent with democratic principles. Although in practice a number of non-intelligence and non-military issues may have an impact on a country's national security—such as food security, climatic conditions, economic inequality and energy security, for example—this is no reason to criminalise holding or dealing with information about such matters.[7]

---

3 Law Council of Australia, *Submission 5*, p. 18; *Submission 5.1*, pp. 1–2; Australian Lawyers for Human Rights, *Submission 7*, p. 5; Human Rights Watch, *Submission 10*, p. 5; Australian Lawyers Alliance, *Submission 12*, p. 5; United Nations Special Rapporteurs, *Submission 30*, p 8; Joint councils for civil liberties, *Submission 31*, pp. 35–38; Nyman Gibson Lawyers, *Submission 35*, pp. 2–3; WWF-Australia, *Submission 36*, p. 1; GetUp, *Submission 38*, p. 2.

4 Australian Lawyers Alliance, *Submission 12*, p. 5.

5 Law Council of Australia, *Submission 5*, p. 18.

6 GetUp, *Submission 38*, p. 2.

7 Australian Lawyers for Human Rights, *Submission 7*, p. 5.

3.9 In response to such concerns, the Attorney-General's Department noted that the reference to 'political, military and economic relations' in section 90.4 of the Bill aligns with the definition of 'international relations' in the *National Security Information (Criminal and Civil Proceedings) Act 2004* (the NSI Act). The Department noted that the NSI Act 'substantially implemented' the recommendations of the 2004 report of the Australian Law Reform Commission (ALRC), *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, which recommended that 'national security information' be defined by reference to the Commonwealth Protective Security Manual that existed at that time and included reference to 'international relations'.[8] The Department added:

> The term is intended to have the same effect as it has in the definition in the NSI Act and to apply broadly to all aspects of a country's relationships with another country in relation to political, military and economic matters.
>
> This covers foreign relations and foreign policy, including a country's strategies for dealing with other nations. It would cover the issues, strategies and methods by which a country seeks to advance its national interests, including with allies, or to protect itself from threats. It would extend to matters involving the country's economic interests, including international negotiations or agreements that may advance a country's economic interests.[9]

3.10 The Department explained that the reference to political and economic relationships could include such matters as:

- information-sharing between governments, including in relation to negotiating positions, strategic outlooks and agency information,
- the confidence or trust held by one government in another government,
- the ability of a government to maintain good working relations with a foreign government, [and]
- a government's reputation or relationships with a foreign government, or between officials.[10]

---

8 Attorney-General's Department, *Submission 6.1*, p. 2; referring to Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information* (Report 98), May 2004.

9 Attorney-General's Department, *Submission 6.1*, p. 45.

10 Attorney-General's Department, *Submission 6.1*, pp. 44–45.

3.11 The Department added at a subsequent hearing that it was 'entirely possible' that the existing espionage offences, which use the term 'security and defence', already cover political and economic relations and that the Bill 'doesn't necessarily narrow or broaden' the offences but rather makes their scope clear.[11]

3.12 At a public hearing, Dr David Neal SC of the Law Council of Australia argued that it was unclear how a court would determine whether or not Australia's political or economic interests have been prejudiced:

> What is it about our political relations with other countries that might be harmed or damaged? And how would a jury conclude beyond a reasonable doubt that publishing an article about the things that he mentioned did or did not prejudice those political relationships, to say nothing of our discussion in public about the economic relations we have with other countries and whether I as a citizen or anyone else as a citizen has the view, 'I think Australia's trade policy with respect to this or that issue is damaging to our economic relationship.'? And then some jury is going to make a conclusion: 'It was,' or 'No, it wasn't'.[12]

3.13 The Law Council noted that it is a 'key component of the rule of law that criminal offences be drafted in a way that's readily known and available, certain and clear'.[13] The Law Council described the concept of national security in the Bill as 'vague', particularly where it extends to preparatory offences and offences involving recklessness.[14] Dr Neal considered that

> parliament really has a responsibility to think whether or not that is an unacceptably broad concept to include as the central concept in an offence that carries a life sentence.[15]

3.14 In a supplementary submission, the Law Council noted that the ALRC's 2004 recommendation for 'national security' to include international

---

11 Ms Tara Inverarity, Assistant Secretary, Attorney-General's Department, *Committee Hansard*, Melbourne, 16 March 2018, p. 44.

12 Dr David Neal SC, Member, National Criminal Law Commission, Law Council of Australia, *Committee Hansard*, Melbourne, 16 March 2018, p. 9.

13 Dr Natasha Molt, Deputy Director of Policy, Law Council of Australia, *Committee Hansard*, Melbourne, 16 March 2018, p. 10.

14 Dr David Neal SC, Member, National Criminal Law Commission, Law Council of Australia, *Committee Hansard*, Melbourne, 16 March 2018, p. 10.

15 Dr David Neal SC, Member, National Criminal Law Commission, Law Council of Australia, *Committee Hansard*, Melbourne, 16 March 2018, p. 14.

relations was in the context of the NSI Act, which is 'largely procedural in nature'. The object of the NSI Act is to

> prevent the disclosure of information in federal criminal proceedings and civil proceedings where the disclosure is likely to prejudice national security, except to the extent that preventing the disclosure would seriously interfere with the administration of justice.[16]

3.15 The Law Council also noted that the breadth of the term 'national security' in the NSI Act is 'balanced by a judicial discretion regarding the administration of justice' and that '[t]here is no such balancing proposed for the espionage, sabotage and foreign interference offences in the [Espionage and Foreign Interference] Bill'.[17]

3.16 The Attorney-General's Department, on the other hand, drew attention to the ALRC's 2009 report *Secrecy Laws and Open Government in Australia*, in which the Commission recommended that the terms 'security' and 'international relations', in the context of secrecy offences, should be defined by reference to the relevant provisions of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) and the NSI Act.[18] The Commission noted that international relations 'has the potential to be interpreted quite broadly', and considered a range of mechanisms for restricting the scope of the provision. However, the ALRC did not recommend such restrictions be implemented and concluded that

> intentional unauthorised disclosure of information that is reasonably likely to damage the international relations of the Commonwealth should be regulated by the criminal law.[19]

3.17 The ALRC added that

> the protection of Australia's international relations is necessary to ensure that Australian society continues to function in the global environment, but a disclosure that merely embarrasses the Australian Government, without threatening real damage to international relations, is unlikely to meet the

---

16 Law Council of Australia, *Submission 5.2*, p. 2; citing *National Security Information (Criminal and Civil Proceedings) Act 2004*, section 3(1).

17 Law Council of Australia, *Submission 5.2*, p. 2.

18 Attorney-General's Department, *Submission 6.1*, p. 44.

19 Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, Report 112, December 2009, p. 153.

> requirements of article 19 of the [International Covenant on Civil and Political Rights].[20]

3.18 The Director-General of Security considered that it was 'very, very defendable' to include political and economic relationships as part of national security, and noted that the definition of national security would change over time:

> One needs to be careful. You can't just sort of lay it down and say, 'That is national security'. It's a very elusive definition. It depends on what is actually a threat to the nation at any given time. And if something is a threat, then I consider that to be part of national security, and it's part of my remit to identify those threats and reflect them to the government, to provide early advice on the threat as it presents.[21]

3.19 In response to a question from the Committee, the Director-General of Security confirmed that, in his view, it is 'absolutely' the case that there is a connection between Australia's diplomatic and economic relations, and its national security, and that harm to diplomatic relations with a foreign country can harm national security.[22]

Meaning of key terms

3.20 The Bill does not define the terms 'espionage', 'sabotage', 'terrorism', 'political violence' or 'foreign interference' for the purpose of the definition of national security in proposed section 90.4. However, the ASIO Act contains similar terms. The definition of 'security' at section 4 of the ASIO Act includes the protection of the Commonwealth, its states and territories and its people from sabotage, espionage, acts of foreign interference and politically motivated violence; and the protection of Australia's territorial and border integrity from serious threats. The ASIO Act:

- does not define sabotage or espionage,
- defines politically motivated violence, and

---

20 Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, Report 112, December 2009, p. 154.

21 Mr Duncan Lewis, Director-General of Security, Australian Security Intelligence Organisation, *Committee Hansard*, Melbourne, 16 March 2018, p. 44.

22 Mr Duncan Lewis, Director-General of Security, Australian Security Intelligence Organisation, *Committee Hansard*, Melbourne, 16 March 2018, p. 45.

- defines acts of foreign interference, which appears similar, but not identical, to the conduct captured by the offences proposed in the Bill.[23]

3.21 The existing sabotage and espionage offences in the Crimes Act and *Criminal Code*, which will be repealed by the Bill, contain definitions for sabotage and espionage as follows:

- 'an act of sabotage' is defined as the 'destruction, damage or impairment, with the intention of prejudicing the safety or defence of the Commonwealth' or certain defence-related articles.[24]
- current espionage offences concern information regarding a country's 'security or defence', which is defined as 'the operations, capabilities and technologies of, and methods and sources used by, the country's intelligence or security agencies'.[25]

3.22 The Attorney-General's Department submitted:

> 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.[26]

3.23 The Explanatory Memorandum provides:

> Because the definition of national security also covers foreign countries, the terms espionage, sabotage, terrorism, political violence and foreign interference are not further defined. This ensures that the terms are not limited by Australian concepts of these matters and are flexible to accommodate the meaning of these terms in foreign countries.[27]

3.24 The Law Council noted that there is an 'element of circularity' in the proposed definition of national security that is likely to make the operation of the sabotage and espionage offence provisions 'unclear and potentially unworkable'. The Law Council recommended that the Bill contain statutory definitions for the terms 'espionage', 'sabotage', 'terrorism', 'political violence' and 'foreign interference'. The Law Council also recommended

---

23 *Australian Security Intelligence Organisation Act 1979*, section 4.

24 *Crimes Act 1914*, section 24AB.

25 *Criminal Code*, section 90.1.

26 Attorney-General's Department, *Submission 6*, p. 14.

27 Explanatory Memorandum, p. 103.

that the terms 'political violence' and 'foreign interference' be defined in a manner consistent with section 4 of the ASIO Act.[28]

3.25 The Attorney-General's Department, however, considered that the terms should not be defined:

> The department is concerned that defining the terms 'espionage', 'sabotage', 'terrorism', 'political violence' and 'foreign interference' by reference to the meaning of these concepts in the Criminal Code and other relevant Commonwealth legislation could limit the utility of the definition when considering the meaning of the national security of a foreign country.[29]
>
> … In the context of Australia's national security, it is possible that a court would interpret the terms ['sabotage', 'espionage' and 'foreign interference'] as being limited to the meaning of the terms as implemented in the offences of the Criminal Code. However, a court may wish to consider a broader interpretation if the ordinary or dictionary meaning is more expansive than the scope of the offences in the Criminal Code.
>
> The department considers that it should be open to a court to find that these terms should be interpreted as broadly as is appropriate, based on the admissible evidence.[30]

3.26 The Department disagreed with a suggestion that the use of the terms 'sabotage', 'espionage' and 'foreign interference' in the definition of national security, which is referred to in the Bill's proposed sabotage, espionage and foreign interference offences, amounted to circular references 'when taken in the context of the whole definition of "national security" and its use in the offences'.[31]

3.27 At a public hearing, the Attorney-General's Department acknowledged that the definition of national security was 'slightly more complex' because of the need for the definition to work in relation to both the national security of Australia and the national security of a foreign country. The Department provided the following explanation as to how the term flows through the Bill:

---

28 Law Council of Australia, *Submission 5*, p. 19.

29 Attorney-General's Department, *Submission 6.1*, pp. 2-3.

30 Attorney-General's Department, *Submission 6.1*, p. 46.

31 Attorney-General's Department, *Submission 6.1*, p. 46.

> The term 'national security' wherever it appears through the act is coupled with something else. It's information concerning national security or where there is a prejudice to national security or an advantage to the national security of a foreign country. So those terms always qualify it in bringing the harm element. It sits in the context of whichever paragraph of the offence it appears in and has meaning in that context, and this is just intended to be that definitive statement of how it flows through. We recognise that it does need some working through, but we do believe it works as a definition for national security with the other acts that seek to in any way grapple with that concept.[32]

3.28 The Inspector-General of Intelligence and Security (IGIS) raised concerns about the lack of statutory definitions of the terms 'sabotage', 'espionage' and 'foreign interference', due to the use of similar terms in the ASIO Act.[33] The IGIS noted that the definition of 'security' in the ASIO Act, which contains the terms sabotage, espionage and foreign interference, is 'pivotal to the exercise of all of ASIOs powers'.[34] The IGIS suggested that this replication could cause confusion:

> Inconsistencies may lead to uncertainty about the scope of ASIO's remit and powers. Such uncertainty is undesirable from a transparency and accountability perspective. If the Parliament's intention is that ASIO's powers in relation to espionage, sabotage and foreign interference should cover matters beyond those criminalised by the proposed provisions, then it would be beneficial for this to be made explicit.[35]

3.29 The IGIS suggested that linking, and limiting, the terms 'espionage' and 'sabotage' in the ASIO Act to conduct covered by the relevant offences in the Bill 'could provide greater certainty and transparency about ASIO's role and the boundaries of its powers'.[36]

3.30 The Attorney-General's Department responded:

> The department does not consider it appropriate for the scope of ASIO's functions to be limited by reference to the meaning of certain terms in the

---

32 Ms Tara Inverarity, Assistant Secretary, Attorney-General's Department, *Committee Hansard*, Melbourne, 16 March 2018, pp. 44–45.

33 Inspector General of Intelligence and Security, *Submission 13*, p. 7.

34 Inspector General of Intelligence and Security, *Submission 13*, p. 6.

35 Inspector General of Intelligence and Security, *Submission 13*, p. 7.

36 Inspector General of Intelligence and Security, *Submission 13*, p. 7.

> criminal law. This is not consistent with ASIO's functions as a security intelligence service.
>
> … To link the definitions to the ASIO Act may have the unintended consequence of limiting the scope of ASIO's powers.[37]

'Prejudice' and 'advantage' of national security

3.31 A number of the proposed espionage, sabotage and foreign interference offences require a person to engage in conduct either with recklessness as to whether their conduct will 'prejudice Australia's national security', or an intention to 'prejudice Australia's national security'.[38] Similarly, a number of the proposed espionage and sabotage offences criminalise conduct undertaken with an intention or recklessness as to whether the person's conduct will 'advantage the national security of a foreign country'.[39] Both of these expressions need to be considered alongside the definition of 'national security', discussed above.

Prejudice to Australia's national security

3.32 The Explanatory Memorandum states that the intention behind using the word 'prejudice' in the Bill is

> to capture a broad range of intended conduct, including an intention to harm or injure Australia's national security or to cause disadvantage to Australia. The term is also intended to cover impairment or loss to Australia's national security interests. The prejudice to Australia's national security is not required to be serious or substantial but is intended to be more than a minor or trivial prejudice that has no long-lasting effect, nor embarrassment to an Australian person or Australia's people.[40]

3.33 GetUp expressed concerns about criminalising conduct that results in 'harm' that is

---

37 Attorney-General's Department, *Submission 6.1*, p. 38.

38 Sabotage offences in sections 82.3(1)(c)(i), 82.4(1)(c)(i), 82.5(1)(c)(i) and 82.6(1)(c)(i); 82.7(d)(i);82.8(d)(i)**;** espionage offences in sections 91.1(1)(c)(i), 91.1(2)(c)(i), 91.2(1)(b), 91.2(2)(b), 91.8(1)(b)(i), 91.8(2)(b)(i); and foreign interference offences in section 92.2(1)(c)(iv), 92.3(1)(c)(iv).

39 Sabotage offences in sections 82.3(1)(c)(ii), 82.4(1)(c)(ii), 82.5(1)(c)(ii) and 82.6(1)(c)(ii); and espionage offences in sections 91.1(1)(c)(ii), 91.1(2)(c)(ii), 91.8(1)(b)(ii), 91.8(2)(b)(ii).

40 Explanatory Memorandum, p 109.

> likely to lead another country or international organisation to lose confidence in the Australian Government, or have a 'detrimental impact' on its working relationship with other countries, or cause reputational damage to the Government.[41]

3.34 The Australian Lawyers Alliance submitted:

> It should not be possible for our government or elected representatives to protect themselves from embarrassment by hiding behind expansive national security provisions. Ultimately, our national security can be enhanced only by ensuring that government is accountable, and that any government misconduct is not hidden from public view.[42]

3.35 Human Rights Watch expressed similar concerns:

> The lack of specificity in what exactly constitutes national security, what 'concerns' national security and how it may be prejudiced, and the very broad definition of what constitutes 'dealing with' information, could mean that any person who receives or communicates political[ly] sensitive information in a public manner could be guilty of one or more espionage offences. Human rights activists and journalists advocating or reporting on politically sensitive arenas would be particularly exposed.
>
> Such standards could easily be used to deter important investigating reporting, since a report or activist will have to guess whether information could be deemed to endanger state security in some undefined way and self-censor, or may even be made liable at a later date for risks the reporter or activist could not possibly be in a position to foresee.[43]

3.36 The Committee sought clarification from the Attorney-General's Department as to whether embarrassment to the Australian government could constitute prejudice to, for example, Australia's political economic or military relations. The Department referred the Committee to the 2009 report of the Australian Law Reform Commission (ALRC), *Secrecy Laws and Open Government in Australia*:

> A disclosure that embarrasses the Australian Government may also cause damage to Australia's international relations. For example, where a disclosure damaged Australia's reputation, as well as being 'embarrassing', it may lead

41 GetUp Australia, *Submission 38*, pp. 2-3.

42 Australian Lawyers Alliance, *Submission 12*, p. 6.

43 Human Rights Watch, *Submission 10*, p. 4.

> to a loss of confidence or trust in Australia. A loss of confidence in the Australian Government's capacity to protect information is likely to result in a restricted flow of information from foreign governments. This, in turn, may impact on Australia's capacity to protect national security or on Australia's capacity to function in the global political, military and economic environment.[44]

3.37 In a supplementary submission, the Department clarified that

> mere embarrassment is not expected to be sufficient to amount to prejudice to Australia's national security. However, there will also be circumstances where embarrassment will lead to the additional consequence of harm being caused to Australia's international relations, for example. If this occurred, it may be possible to prove, beyond a reasonable doubt, that there was prejudice to Australia's national security.[45]

Advantage the national security of a foreign country

3.38 The Bill does not define the term 'advantage' and as such the term will be given its ordinary meaning. The Macquarie dictionary defines 'advantage' as 'to be of service to; yield profit or gain to; benefit'.[46]

3.39 In some instances, the Explanatory Memorandum appears to indicate that 'advantage' requires there to be a benefit to the foreign country's national security relative to Australia's national security:

> The term 'advantage' is intended to capture an intention to put another country's national security in a favourable or superior position compared to Australia's position or to benefit or profit another's country's national security compared to Australia's national security.[47]

3.40 In other instances, the Explanatory Memorandum describes the intention of the term 'advantage' without any reference to Australia's security:

---

44 Attorney-General's Department, *Submission 6.1*, p. 48; citing Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, 2009, para 5.45.

45 Attorney-General's Department, *Submission 6.3*, p. [3].

46 See <https://www.macquariedictionary.com.au/features/word/search/?word=advantage&search_word_type=Dictionary> viewed 21 March 2018.

47 Explanatory Memorandum, pp. 47, 51, 59, 135, 139.

> The term 'advantage' is intended to capture an intention to put another country's national security in a favourable or superior position than it would have been without the communication of this information.[48]

3.41 The Committee asked the Department if it could be possible to 'advantage the national security of a foreign country', for example one of Australia's allies, without detrimentally affecting Australia's national security, suggesting that the conduct the Bill should seek to deter only be that conduct that detrimentally affects Australia's national security. The Department answered by reference to the proposed espionage offences (discussed in Chapter 6):

> If a person is advantaging the national security of one of Australia's allies, the defence at subsection 91.4(1) would apply.
>
> The department notes that, to [the] extent this is an issue, it would also be an issue with the existing espionage offences. The structure of the existing offence at subsection 91.1(2) of the Criminal Code has been replicated, with the exception of casting the matter of 'lawful authority' as a defence rather than as an element of the offence.[49]

Definition of 'foreign principal'

3.42 The term 'foreign principal' is defined in proposed section 90.2 of the *Criminal Code*. The Bill's definition of 'foreign principal' differs from the definition in the Foreign Influence Transparency Scheme Bill 2017 (FITS Bill), in that it does not include private businesses or individuals. However, the term does include:

- a foreign government principal,
- a public international organisation,
- a terrorist organisation, and
- an entity or organisation owned, directed or controlled by one or more foreign government principals, public international organisations or terrorist organisations.

3.43 The definition of 'foreign principal' underpins many of the proposed sabotage, espionage and foreign interference offences. A consistent element of these offences is undertaking certain activities on behalf of, in support of,

---

48 Explanatory Memorandum, pp. 109, 114.

49 Attorney-General's Department, *Submission 6.1*, p. 47.

in collaboration with, or as directed by a foreign principal. Furthermore, the theft of trade secrets offence is limited to conduct undertaken on behalf of, in support of, in collaboration with, or as directed by a 'foreign government principal'.

3.44 The term 'foreign government principal' is defined at proposed section 90.3 to include foreign governments and their authorities; foreign local government and regional government bodies; foreign public enterprises; foreign political organisations; and other entities owned, directed or controlled by one or more foreign government principals.

3.45 The term 'public international organisation' is defined at existing section 70.1 of the *Criminal Code* and includes multi-lateral organisations such as the World Bank, the Word Trade Organisation and the International Monetary Fund. The Explanatory Memorandum states that the provision of information to such organisations could prejudice Australia's national security and constitute espionage in some situations:

> For example, Person I is an official of International Organisation Z and obtains confidential information concerning a significant impending change in Australia's economic policies from Person J, an Australian official who intends to harm Australian interests for ideological reasons. International Organisation Z uses this information to undermine Australia's position in multilateral trade negotiations, causing significant damage to Australia's international relationships.[50]

3.46 The term 'terrorist organisation' is defined at existing section 102.1 of the *Criminal Code* as 'an organisation that is directly or indirectly engaged in, preparing, planning, assisting in or fostering the doing of a terrorist act' or an organisation that is specified by the regulations.

3.47 The Attorney-General's Department explained the reasoning behind the difference in definition of foreign principal between this Bill and the FITS Bill:

> It would not be appropriate for the definition of 'foreign principal' for the purposes of the serious criminal offences in this Bill to be as broad as the definition for the FITS Bill, which aims to bring transparency to foreign influence in Australia's political and governmental processes.
>
> It would be inappropriate, for example, to extend espionage offences to conduct undertaken on behalf of a foreign business or foreign individual.

---

50 Explanatory Memorandum, p. 99.

> These offences are limited to conduct undertaken on behalf of foreign countries and a limited range of non-state actors.[51]

3.48 Some participants raised concerns that the definition of foreign principal would extend the Bill's offences to information provided to the United Nations and its subsidiary bodies, or other international organisations that work independently of governments.[52]

3.49 GetUp argued that the Bill should be revised to 'narrow the definition of 'foreign principal' to include only foreign governments and their agents'.[53]

3.50 These concerns appear to also arise in relation to Australia's existing espionage laws, which apply where a person communicates or makes available information to either 'another country' or a 'foreign organisation', or to 'a person acting on behalf of such a country or organisation'.[54]

3.51 The Australian Lawyers Alliance was concerned about the lack of specificity in the definition of 'foreign political organisation', which, as part of the definition of foreign government principal, it considered was 'fundamental in determining whether offences under the proposed reforms have been committed'.[55] The term 'foreign political organisation' is defined at proposed subsection 90.1(1) as being 'a foreign political party or a foreign political organisation'. No further explanation is included in the Explanatory Memorandum, other than to say that it 'will include political parties of foreign countries'.[56]

3.52 The Alliance noted:

> There are many international organisations, such as companies, news outlets and international non-government organisations, which engage in research, reporting and advocacy around specific themes. Facebook and Google, for example, made submissions to the ongoing inquiry into public interest journalism. The Guardian (a UK-based news outlet) and the New York Times

---

51 Attorney-General's Department, *Submission 6.1*, p. 50.

52 Law Council of Australia, *Submission 5.1*, p. 3; Australian Lawyers Alliance, *Submission 12*, pp. 7-8; GetUp, *Submission 38*, p. 2; Dr David Neal SC, Member, National Criminal Law Commission, Law Council of Australia, *Committee Hansard*, Melbourne, 16 March 2018, p. 15.

53 GetUp Australia, *Submission 38*, p. 3.

54 *Criminal Code*, section 91.1.

55 Australian Lawyers Alliance, *Submission 12*, p. 7.

56 Explanatory Memorandum, p. 97.

> (a USA-based news outlet) each have Australian bureaux that regularly report on Australian domestic politics and Australia's place in the world. International human rights organisations, such as Amnesty International and Human Rights Watch, each have an Australian presence and seek to influence Australian government policy, despite operating global funding models independent of governments. The United Nations also regularly comments on Australia's implementation of its obligations under international law.
>
> … These organisations can be based, or receive funding from, abroad but do not represent the interests of any foreign government or political party. Despite this, however, it is possible for them to be caught up in the offences created by the Bill, due to the broad nature of the definitions.[57]

3.53 The Alliance recommended that definition be 'more closely aligned with the need to protect Australia's national security' by

> limiting the definition of foreign political organisations to foreign governments, foreign political parties and organisations aligned with such governments or parties. Alternatively, drafters could consider adding a clarification that the provisions are not designed to capture the United Nations, media organisations, companies or NGOs that work independently of governments.[58]

3.54 In relation to the application of the Bill to entities that are 'owned, directed or controlled' by foreign public enterprises, local or regional government bodies and foreign political organisations, the Attorney-General's Department stated:

> If the definition did not cover these entities, it would be very easy for a foreign principal to avoid the application of the offences by simply, for example, running their espionage activities through another company that the entity owns or controls.[59]

Definition of 'foreign intelligence agency'

3.55 The Bill defines 'foreign intelligence agency' as 'an intelligence or security service (however described) of a foreign country'.[60] The Dictionary to the Criminal Code defines foreign country to include:

---

57 Australian Lawyers Alliance, *Submission 12*, pp. 8–9.

58 Australian Lawyers Alliance, *Submission 12*, p. 9.

59 Attorney-General's Department, *Submission 6.1*, p. 50.

60 Schedule 1, item 24.

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

3.56 The Explanatory Memorandum states:

> The definition of 'foreign intelligence agency' is intentionally broad to capture the range of intelligence agencies that exist in various countries. Such agencies will generally, but not always, have comparable functions to agencies in the Australian Intelligence Community, as set out at the definition of domestic intelligence agency in section 121.1 of Schedule 2 of this Bill.

3.57 Proposed section 121.1 in the Bill defines domestic intelligence agency as:

- 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.

3.58 The Law Council raised concerns with the proposed definition of 'foreign intelligence agency':

> The Law Council is concerned that the proposed definition of a 'foreign intelligence agency' does not sufficiently define by criteria what may amount to an intelligence or security service of a foreign country. For example, it is not clear whether a foreign trade or economics agency may be considered an intelligence or security service (however described) of a foreign country.[61]

3.59 The Law Council suggested that the Bill could provide a criteria to determine whether a service is a 'foreign intelligence agency' by drawing on existing Commonwealth laws:

> [T]he Law Council considers that a 'foreign intelligence agency' should be defined to mean (for example) an entity that is directed or controlled by a foreign government or governments that has responsibility for: intelligence about the capabilities, intentions or activities of people or organisations outside Australia; or the security of a foreign country. If it is thought necessary to extend this definition to non-State actors, a reference could be made to a

61 Law Council of Australia, *Submission 5*, p. 25.

> foreign political organisation. However, there must also be a link to harm or prejudice to Australia's national security in the offence provisions.[62]

3.60 The Attorney-General's Department did not consider it necessary for the definition to align with other Commonwealth legislation, 'as the terms properly take different meaning in different contexts'.[63] Further, the Department argued:

> A definition along the lines of an 'entity that is directed or controlled by a foreign government or governments that has responsibility for gathering security or defence intelligence about the capabilities, intentions or activities of people or organisations outside its own territory' would be more challenging to prove than the definition set out in the Bill and undermine the efficacy of the offences.
>
> There is no intention to cover non-State actors in this definition. It is limited to agencies of foreign countries.[64]

Definition of 'Australian Government security clearance'

3.61 A number of the aggravated offences proposed by the Bill will arise in connection to an 'Australian Government security clearance':

- aggravated espionage offences;[65]
- aggravated secrecy offences;[66] and
- the aggravated offence for giving false or misleading information.[67]

3.62 The proposed aggravated espionage and secrecy offences arise where a person holds an Australian Government security clearance at the time of committing the underlying offence. The aggravated offence for giving false or misleading information will arise where a person gives false or misleading information in connection with the application for, or the maintenance of, an Australian Government security clearance (regardless of

---

62 Law Council of Australia, *Submission 5*, p. 26.

63 Attorney-General's Department, *Submission 6.1*, p. 5.

64 Attorney-General's Department, *Submission 6.1*, p. 5.

65 Proposed section 91.6(b)(v). The aggravated espionage offences only apply to Subdivision A espionage offences.

66 Proposed section 122.3(1)(b)(v)

67 Proposed section 137.1A.

whether the person is the holder or applicant for a security clearance, or is some other person providing information as part of that process).

3.63 The term 'Australian Government security clearance' is not defined in the Bill. The Explanatory Memorandum states that the term 'Australian Government security clearance':

> … is intended to capture security clearances granted by the Australian Government Security Vetting Agency or another government agency conducting and issuing security clearances under the Protective Security Policy Framework. It would capture, for example, security clearances from Baseline to Top Secret Positive Vetting level.[68]

3.64 The Australian Government's Protective Security Policy Framework includes four security clearance levels:

- Baseline: enabling the clearance holder to access information up to and including PROTECTED information,
- Negative Vetting Level 1: enabling the clearance holder to access up to and including SECRET information;
- Negative Vetting Level 2: enabling the clearance holder to access up to and including TOP SECRET information; and
- Positive Vetting: enabling the clearance holder to access TOP SECRET information and certain sensitive, caveated, compartmented and code-word information'.[69]

3.65 A number of state, territory and federal government employees, as well as certain other persons working with government, require a security clearance.

Secrecy-related definitions

3.66 Concerns were raised during the inquiry about the definitions of the terms 'inherently harmful information' and 'causing harm to Australia's interests' in relation to the secrecy offences in Schedule 2. These issues are discussed in Chapter 4.

---

68 Explanatory Memorandum, p. 132 and p. 271.

69 Attorney-General's Department, *Australian Government Personnel Security Protocol* (version 2.3), p. 16.

Committee comment

National security

3.67 The Committee notes concerns raised by participants in the inquiry about the breadth of the definition of 'national security' in proposed section 90.4. In particular, participants expressed concerns about national security including political or economic relations with other countries, and the potential for offences that rely on these terms to impact on freedom of expression. Concerns have also been raised about the level of ambiguity in the definition.

3.68 Many of the proposed new offences in the Bill include 'prejudice Australia's national security' and/or 'advantage the national security of a foreign country' as a key element in determining whether a person is culpable under the offence. This includes a range of proposed offences for espionage, foreign interference and sabotage that are discussed later in this report. The Committee therefore considers it essential that the term 'national security' is clear, unambiguous and appropriately targeted.

3.69 The Committee notes that the inclusion of a country's 'political, military or economic relations' in the Bill's definition of national security is intended to align with the *National Security Information (Criminal and Civil Proceedings) Act 2004*, which defines national security as 'Australia's defence, security, international relations or law enforcement interests'. The Committee also notes that the ALRC recommended that these matters be included in the general secrecy offence in the *Criminal Code*, considered whether the scope of these matters should be restricted in any way in light of their 'potential to be interpreted quite broadly', and concluded that they should not be so restricted. The ALRC considered that the protection of Australia's international relations at criminal law was consistent with Australia's international obligations under the International Covenant on Civil and Political Rights (ICCPR) on the basis that it was necessary to ensure that Australian society continues to function in the global environment.

3.70 The Committee considers that there are some circumstances in which it is would be appropriate to include an impact on international relations as an element of a criminal offence. For example, it may be appropriate that certain foreign interference offences capture instances where a foreign

power engages in covert or deceptive conduct, or makes threats of serious harm, in order to prejudice Australia's economic or political relationships.

3.71 The Committee notes some concerns about the threshold of the expression 'prejudice Australia's national security' that is proposed in the Bill. In particular, witnesses expressed concern that embarrassment to government could be sufficient to satisfy prejudice to national security—and in particular to international relations.

3.72 The Committee recognises that, in some circumstances, embarrassment to the Australian Government could result in harm to Australia's political, military or economic relationships. However, the Committee considers that greater clarity is required to ensure that prejudice cannot consist of embarrassment to the Australian Government or other Australian entity alone, but must also include a degree of damage or harm.

Recommendation 2

3.73 The Committee recommends that the Bill be amended to clarify that, for the purpose of the Bill's espionage, foreign interference and sabotage offences, the expression 'prejudice to national security' cannot consist of

- **embarrassment alone, and**
- **must also include a degree of damage or harm.**

3.74 Similarly, the Committee considers that further legislative clarity is required to reduce the likelihood of non-malicious conduct falling under the term 'advantage the national security of a foreign country' for the purposes of the proposed sabotage and espionage offences.

3.75 The explanation of this term currently varies within the Explanatory Memorandum. However, the Committee considers it would be inappropriate to criminalise activity that is undertaken for the mutual benefit of both Australia and a foreign country.

Recommendation 3

3.76 The Committee recommends that the Bill be amended to reflect the intent of the Explanatory Memorandum that the term 'advantage the national

security of a foreign country' does not apply to conduct that is mutually advantageous to the security of both Australia and the foreign country.

3.77 The Committee notes concerns about the need for clarity with respect to certain key terms within the definition of national security, including 'sabotage', 'espionage', 'foreign interference' and 'political violence'. Clarity in the criminal law is of great importance.

3.78 The Committee also notes the evidence of the Attorney-General's Department that including statutory definitions of these terms could limit the applicability of the offences in relation to persons engaging in conduct, such as espionage, to advantage the national security of a foreign country. In this respect, the Committee recognises that a key imperative underpinning this Bill is that foreign countries have very different conceptions of the 'appropriate' role for espionage and their intelligence services, for example extending to the use of their intelligence services to interfere with democratic elections, or to coerce diaspora communities in Australia and other countries. It would, therefore, be important that the offences in the Bill not be limited in their application to what Australia or other Western countries might traditionally regard as 'espionage' or 'foreign interference'.

3.79 The Committee also received evidence from the Director-General of Security that foreign intelligence services seek to structure their activities to exploit gaps in Australia's legislative framework.

3.80 Accordingly, the Committee considers that it would be beneficial to amend the Explanatory Memorandum to include more, and more specific, detail about what is meant by the terms 'sabotage', 'espionage', 'foreign interference' and 'political violence'. However, it should be a matter for the courts to interpret these terms, in light of all of the admissible evidence.

Recommendation 4

3.81 The Committee recommends that the Explanatory Memorandum be amended to provide greater clarity about the intended meaning of the terms 'espionage', 'sabotage', 'political violence' and 'foreign interference' for the purposes of the definition of national security at proposed section 90.4.

3.82 The Committee notes the intent of the Bill is not to affect the operation of any existing provisions in the ASIO Act. However, due to Bill's use of

similar or identical terms to those existing in the ASIO Act, the Committee considers that the Bill should be amended to make this intention clear.

Recommendation 5

3.83 The Committee recommends that the Bill be amended to clarify that the Bill does not affect the operation of existing provisions in the *Australian Security Intelligence Organisation Act 1979*, unless explicitly stated.

Foreign principal

3.84 The Committee notes concerns raised by some participants in the inquiry about the potential breath of the definition of 'foreign principal'. The definition of this term is important for the proposed offences of espionage (which involve making information available to a foreign principal), foreign interference (which involves conduct on behalf of a foreign principal) and sabotage (which may involve conduct on behalf of a foreign principal). Additionally, the proposed 'theft of trade secrets' offence includes conduct undertaken on behalf of a 'foreign government principal'.

3.85 The Committee considers it appropriate that the term 'foreign principal' is more narrowly defined in the Bill than the equivalent term in the Foreign Influence Transparency Scheme Bill 2017.

3.86 However, the Committee notes that there remains some ambiguity about the scope of the term. In particular, the Committee notes the lack of clarity in relation to 'foreign political organisation' as part of the definition of 'foreign government principal'. While the Bill and its Explanatory Memorandum make clear that foreign political parties are part of the definition of foreign political organisations, it is unclear what other organisations may be considered to be foreign political organisations. The Committee considers that this ambiguity should be rectified.

3.87 The Committee considers that it would be inappropriate for organisations that have no connection to a foreign government or foreign political party to be included as part of the definition of 'foreign government principal'. Accordingly, the Committee recommends that the Bill be amended to provide greater clarity about what kinds of foreign political organisations may be covered.

Recommendation 6

3.88 The Committee recommends that the Bill be amended to define what foreign political organisations may be covered by the term 'foreign political organisation'.

3.89 The Committee also notes that 'foreign principal' is proposed to include 'foreign international organisations', such as the World Bank, the World Trade Organisation and the International Monetary Fund. The Committee notes that this would include a range of multilateral organisations of which Australia is a member, including the United Nations and its subsidiary bodies. The Explanatory Memorandum includes a hypothetical example of a person providing confidential information to an international organisation in order to undermine Australia's position in multilateral trade negotiations.

3.90 The Committee is conscious of concerns raised by some submitters about the potential for offences in the Bill to capture information reported to international bodies, such as the United Nations Human Rights Committee. It is important that members of civil society be able to engage with public international organisations on matters of public importance.

3.91 However, the Committee notes the Attorney-General's Department's evidence that the offences that involve the communication of information about Australia's national security, including its political or economic relations, are also 'coupled' with additional elements that qualify their scope to apply to harmful conduct.[70] The Committee is also conscious of the evidence of the Director-General of Security and the Department as to the risks in introducing significant gaps into the legislative framework that would be open to exploitation by foreign intelligence services. Additionally, as noted above, the current espionage offences in the Criminal Code apply to persons who communicate information to foreign organisations, and the Department has given evidence that these offences may well apply to persons who communicate information that prejudices Australia's international relations.

3.92 In the Committee's view, it would not be desirable to narrow the existing espionage offences to exclude public international organisations. To do so would incentivise foreign intelligence services to channel their espionage

---

70 Ms Tara Inverarity, Assistant Secretary, Attorney-General's Department, *Committee Hansard*, Melbourne, 16 March 2018, p. 45.

activities through such organisations, undermining the efficacy of the legislative framework.

Australian Government security clearance

3.93 The Committee notes that the term 'Australian Government security clearance' is not currently defined in the Bill. Although the intention of the term is made clear in the Explanatory Memorandum, to provide greater certainty the Committee considers that the meaning of an 'Australian Government security clearance' should be defined within the Bill.

Recommendation 7

3.94 The Committee recommends that the Bill be amended to define the meaning of 'Australian Government security clearance'.

Security classifications

3.95 The Bill proposes a number of secrecy and espionage offences that are premised on dealings with information or an article that 'has a security classification'.[71] The Bill also creates a number of aggravated espionage and secrecy offences connected to security classifications.[72] For all of these offences, criminal liability is triggered by the existence of the security classification itself, rather than the substance or quality of the underlying information. The offences and aggravated offences do not require that the dealing with the information caused any harm, only that the information

---

71 Proposed espionage offences in sections 91.1; 91.1(2), 91.3. Proposed secrecy offences in sections 122.1(1), 122.1(2), 122.1(3) and122.1(4) arise in relation to conduct involving 'inherently harmful information', a subset of which is information that has a security classification (refer to the definitions of 'inherently harmful information' and 'security classified information' in section 121.1)

72 Aggravated espionage offences arise where any of the following circumstances exist: the information 'has a security classification of secret or above' (91.6(b)(i)); the person dealt with five or more records or articles each of which has a security classification (91.6(b)(iii)); or the person altered a record or article to remove or conceal its security classification (91.6(b)(iv)).

Similarly, aggravated secrecy offences arise where any of the following circumstances exist: the information 'has a security classification of secret or above' (122.3(b)(i)); the person dealt with five or more records or articles each of which has a security classification (122.3(b)(iii)); or the person altered a record or article to remove or conceal its security classification (122.3(b)(iv)).

possessed the requisite security classification. The relevant offences attract penalties ranging from five years' imprisonment up to life imprisonment.

3.96 The Bill does not define the term 'security classification', but proposes prescribing the meaning of this phrase in regulations.[73] The regulations are yet to be developed.[74]

3.97 Submitters raised concerns with the use of security classifications as the basis for criminal offences.[75] Submitters identified the key difficulties as:

- the proposal to define the term 'security classification' in regulations,
- the use of an administrative system for document management as the basis of criminal liability, and
- the use of strict liability and evidentiary certificates.

Regulations

3.98 Various submitters raised concerns about the proposal for the meaning of 'security classification' to be prescribed in regulations.[76] The Bill does not provide guidance as to what classification categories will be included, or what types of information the regulations could prescribe as classified, other than a requirement that 'the Minister must be satisfied that the regulations are not inconsistent with the policies of the Government of the Commonwealth in relation to protective security'.

3.99 Although the Bill does not provide this detail, the Explanatory Memorandum states:

> It is anticipated that the regulations will prescribe the relevant protective markings that will denote information as being classified for the purpose of these offences. At this time, these markings are listed in the *Australian Government information security management guidelines – Australian Government security classification system* … and include:
>
> - PROTECTED
> - CONFIDENTIAL

---

73 Proposed section 90.5.

74 Attorney-General's Department, *Submission 6.1*, p. 54.

75 Law Council of Australia, *Submission 5;* Human Rights Law Centre, *Submission 7*.

76 Law Council of Australia, *Submission 5,* pp. 21–22; Human Rights Law Centre, *Submission 11*, p. 21; Valerie Heath, *Submission 14*, p. 2; Australian Human Rights Commission, *Submission 17*, p. 4; Joint councils for civil liberties, *Submission 31*, p. 12; Valerie Heath, *Submission 14*, p. 2.

- SECRET
- TOP SECRET.[77]

3.100 The *Australian Government information security management guidelines – Australian Government security classification system* (the Guidelines) provide that when information is created, the originator should assess the consequences of unauthorised compromise or misuse of the information and classify the information accordingly.[78] Where compromise of the confidentiality of information could be expected to cause damage to the 'national interest', organisations or individuals the originator should classify the information PROTECTED. The information should be classified CONFIDENTIAL where that damage would be 'significant' and SECRET where that damage would be 'serious'.[79]

3.101 Information should be classified TOP SECRET only where compromise of the confidentiality of information could be expected to cause exceptionally grave damage to the 'national interest'.[80]

3.102 The phrase 'national interest' has broader scope than 'national security'—the Guidelines provide that national security is a subset of 'national interest'. National security is the protection from espionage, sabotage, politically motivated violence, promotion of communal violence, attacks on Australia's defence system, acts of foreign interference and the protection of Australia's territorial and border integrity from serious threats and defence capability.[81] 'National interest information' also captures any 'official resource' concerning Australia's:

- international relations, significant political and economic relations with international organisations and foreign governments
- law and governance, including:

---

77 Explanatory Memorandum, p. 104.

78 Australian Government, *Information security management guidelines – Australian Government security classification system*, p. 4.

79 Australian Government, *Information security management guidelines – Australian Government security classification system*, p. 9.

80 Australian Government, *Information security management guidelines – Australian Government security classification system*, p. 9.

81 Australian Government, *Information security management guidelines – Australian Government security classification system*, pp. 6–7.

  - interstate/ territory relations
  - law enforcement operations where compromise could hamper or make useless national crime prevention strategies or particular investigations, or endanger personal safety
- economic, scientific or technological matters vital to Australia's stability, integrity and wellbeing
- heritage or culture.[82]

3.103 Although the Attorney-General's Department indicated its intention that the term 'security classification' would take its meaning from the Guidelines outlined above, submitters were concerned that this content is not prescribed in the Bill itself.[83] The joint councils for civil liberties submitted that this approach would allow very low level security classified information to be criminalised, even though the communication of this information would cause no harm to Australia's interests.[84]

3.104 The Human Rights Law Centre submitted that the government's current document classification framework is 'supplemented and may in some instances be overridden by policies developed by each governmental agency', which would not necessarily be made publicly available.[85] The Human Rights Law Centre described this as

> a certainty-of-law issue, which comes to the sort of precision that we want to see in our criminal law. If we are creating offences with such severe penalties, we need to be confident that the way in which those laws are drafted captures circumstances where those penalties are appropriate. … if this is going to be an offence introduced into our Criminal Code on an enduring basis, parliament needs to be satisfied that those documents will continue to be classified in a way that is appropriate, such that disclosure of them or handling of them gives rise to this sort of criminal offence. It's very hard to do

---

82 Australian Government, *Information security management guidelines – Australian Government security classification system*, p. 7.

83 Law Council of Australia, *Submission 5,* p. 21; Joint councils for civil liberties, *Submission 31*, p. 12; Mr Edward Santow, Human Rights Commissioner, Australian Human Rights Commission, *Committee Hansard,* Canberra, 31 January 2018, p. 48.

84 Joint councils for civil liberties, *Submission 31*, p. 12; Valerie Heath, *Submission 14*, p. 13.

85 Human Rights Law Centre, *Submission 11*, p. 21.

> that if the administrative classification is itself not governed by law in any way.[86]

3.105 The Australian Human Rights Commission was similarly concerned, submitting that:

> … to the extent that a person (or category of persons) is unable to inform themselves prospectively of the specific conduct that is prohibited in order to avoid falling foul of [an offence], the Bill violates a core principle of the rule of law.[87]

3.106 The Human Rights Commissioner noted that 'what's considered classified can change via regulation with, obviously, less transparency and without full parliamentary oversight'.[88]

3.107 The Attorney-General's Department advised that there 'is no intention to allow for documents that are not publicly available to be incorporated into the definition' and that the Bill could be amended to make this a requirement.[89]

3.108 The IGIS suggested that consideration could be given to including parameters for the term 'security classification' in the primary legislation, noting that:

> The lack of transparency about the basis for classifications and the absence of any requirement as to the purpose of classification leaves open the risk, or at least the perception, that documents may be classified or over-classified for purposes such as avoiding public disclosure of politically inconvenient information or information about illegal or improper activities of intelligence agencies.[90]

3.109 The Law Council similarly recommended:

> The type of information which may be prescribed as 'security classified information' should be clearly defined and circumscribed in the Bill, for

---

86 Dr Aruna Sathanapally, Director Legal Advocacy, Human Rights Law Centre, Canberra, *Committee Hansard*, Melbourne, 16 March 2018, p. 22.

87 Australian Human Rights Commission, *Submission 17*, p. 4.

88 Mr Edward Santow, Human Rights Commissioner, Australian Human Rights Commission, *Committee Hansard,* Canberra, 31 January 2018, p. 48.

89 Attorney-General's Department, *Submission 6.1,* p. 39.

90 Inspector-General of Intelligence and Security, *Submission 13,* p. 8.

example, through appropriate criteria to assist in ensuring that the matter would, or would be reasonably likely to, cause harm to or prejudice Australia's national security.[91]

Appropriateness as a threshold for criminality

3.110 Participants in the inquiry raised concerns regarding the use of administrative document management guidelines as the basis for criminal liability. Submitters raised concerns that:

- documents are routinely 'over-classified' or classified incorrectly;
- classification decisions are not re-evaluated over time;
- the approach is not harm-based; and
- the Bill does not implement a mechanism to test the appropriateness of document classifications.

3.111 The Human Rights Law Centre submitted that the process of classifying information is guided by non-mandatory guidelines, which allow individual departments to take different approaches.[92] The Centre submitted:

> This intuitively makes sense given that they face different situations, but the consequence of that is that security classification is not law governed.
>
> Security classification does not exist in legislation and there is no situation by which an individual officer giving a particular security classification to a document will necessarily have anyone sign off on that. So, given that security classification exists for a particular purpose, taking it and putting it in criminal law has real difficulties because it doesn't have the checks and balances that you would have around something that would give rise to criminal responsibility. Just to make it really simple, you could have the consequence where a single public servant at a junior level could make a call about a security classification of a document and thereby create something that triggers a criminal offence under the Criminal Code. In terms of the way in which our legal system operates, that's not good law.[93]

3.112 In contrast, the Explanatory Memorandum states:

---

91 Law Council of Australia, *Submission 5,* p. 8.

92 Dr Aruna Sathanapally, Director Legal Advocacy, Human Rights Law Centre, Canberra, *Committee Hansard*, Canberra, 30 January 2018, p. 58.

93 Dr Aruna Sathanapally, Director Legal Advocacy, Human Rights Law Centre, Canberra, *Committee Hansard*, Canberra, 30 January 2018, p. 58.

> The Commonwealth has well-established processes for determining whether particular information has been properly security classified, or remains appropriately security classified.[94]

3.113 The Attorney-General's Department submitted:

> Assessments about the appropriate security classification are made by officers with the relevant knowledge and expertise in the subject-matter and context. For example, a classification of TOP SECRET should be applied if the compromise of the confidentiality of information could be expected to cause exceptionally grave damage to the national interest. The application of a security classification therefore indicates that an appropriately qualified person has made an assessment of the harmfulness of the information.[95]

3.114 In contrast, a number of participants expressed concern that the practical reality of governmental document classification is that documents are routinely 'over-classified'.[96] The IGIS similarly submitted that the process of governmental document classification is 'not a precise science'. She advised:

> As Inspector-General, I frequently see documents that appear to be over-classified or documents that may have been correctly classified when created but would now warrant a lower classification because of the passage of time or authorised public disclosure of related information.[97]

3.115 The IGIS considered that the 'tendency to over-classify documents "to be safe" is understandable', noting that the 'main things' presently hinging on security classifications are the procedures that need to be applied to store, transport, destroy and disseminate the information.[98]

---

94 Explanatory Memorandum, p. 229.

95 Attorney-General's Department, *Submission 6.1*, p. 37.

96 Human Rights Law Centre, *Submission 11*, p. 22; United Nations Special Rapporteurs (on the promotion and protection of the right to freedom of opinion and expression; on the promotion and protection of human rights and fundamental freedoms while countering terrorism; and on the situation of human rights defenders), *Submission 30*; Joint councils for civil liberties, *Submission 31*, p. 13; Mr Edward Santow, Human Rights Commissioner, Australian Human Rights Commission, *Committee Hansard,* Canberra, 31 January 2018, p. 49.

97 Inspector-General of Intelligence and Security, *Submission 13,* p. 7.

98 Inspector-General of Intelligence and Security, *Submission 13,* p. 7

3.116 One submission stated that it would be disingenuous to suggest that the Commonwealth has a consistent, robust or reliable methodology that it applies in classifying information:

> While some classification guides exist pertaining to particular types of information, and some agencies have more mature processes than others, security classifications are for the most part assigned arbitrarily by the creator of a piece of information.
>
> … It is very common in the intelligence agencies to over classify even the most trivial of information. Reports derived almost entirely from unclassified, open source material, which are not the result of any novel or sensitive analytical techniques, and which if disclosed would have no impact to Australia's security or defence are routinely assigned very high level classifications, for no discernible reason.
>
> Even an email invitation to a social event, such as a trip to the pub after work, or to a farewell party for a departing colleague will often be classified at the TOP SECRET codeword level. This is because it is a common habit to assign the maximum possible classification to everything by default, rather than because disclosure of the information in question actually presents any risk to the security or defence of Australia.[99]

3.117 The submission added that due to the 'serious personal consequences' that could result from an individual under-classifying information, including loss of employment in extreme cases, the 'safe and most prudent option is to always over classify'.[100] The joint councils for civil liberties similarly noted that there 'are no repercussions for over-classification in the guidelines or legislation'.[101]

3.118 The United Nations Special Rapporteurs noted that the Guidelines published by the Attorney-General's Department are 'implemented and enforced without judicial review or oversight'.[102]

---

99 *Submission 26* (name withheld), p. [1].

100 *Submission 26* (name withheld), p. [1].

101 Joint councils for civil liberties, *Submission 31*, p. 13.

102 United Nations Special Rapporteurs (on the promotion and protection of the right to freedom of opinion and expression; on the promotion and protection of human rights and fundamental freedoms while countering terrorism; and on the situation of human rights defenders), *Submission 30*, p. 5.

3.119 At a public hearing, the Attorney-General's Department outlined the rationale for premising criminality on the existence of a security classification, rather than the substance of the underlying material:

> What we've been trying to achieve with the security classification is that it's not up to the individual to decide whether that classification is right or wrong. It's not for me to decide whether a document I receive from an intelligence agency has been correctly classified or if I believe it's been overclassified to release it to somebody else. It's essential, particularly when you are talking about malicious insiders, that it is not up to the individual to decide whether that security classification is right or wrong. The fact that it was classified by the originating agency is what matters, because that is the agency that has the access to all of the contextual information that must be taken into account in deciding whether that classification should be applied.[103]

3.120 Submitters were also concerned that there is no mandatory process for declassifying documents. This means that, even where a document is correctly classified at the time that it is authored, by the time it is dealt with, that classification may no longer be appropriate.[104] The Attorney-General's Department stated:

> If a person wishes to disclose information that has that classification—say, if it's a historical document and they hold a genuine view that it does not still carry that harm—they should be speaking to the originating agency about declassifying it. If the originating agency doesn't agree with that, they should not be disclosing that document.[105]

3.121 Noting their objection to the use of security classifications as a basis for criminal liability, the Human Rights Law Centre suggested that if the offences were to proceed

> there would need to be a process to confirm that security classification is correct, not just that it existed, before prosecution were commenced.[106]

---

103 Ms Tara Inverarity, Assistant Secretary, Attorney-General's Department, *Committee Hansard*, Canberra, 31 January 2018, p. 29.

104 Human Rights Law Centre, *Submission 11*, p. 22; Joint councils for civil liberties, *Submission 31*, p. 13.

105 Ms Tara Inverarity, Assistant Secretary, Attorney-General's Department, *Committee Hansard*, Melbourne, 16 March 2018, p. 60.

106 Dr Aruna Sathanapally, Director Legal Advocacy, Human Rights Law Centre, Canberra, *Committee Hansard*, Canberra, 30 January 2018, p. 57.

3.122 The Law Council of Australia recommended that the Bill should, at a minimum, contain a provision similar to that which exists in section 50A of the *Australian Border Force Act 2015*.[107] Section 50A provides that

> proceedings for the offence must not be initiated unless the Secretary has certified that it is appropriate that the information had a security classification at the time of the conduct that is alleged to constitute the offence'.

3.123 At the time section 50A was introduced, the accompanying Explanatory Memorandum provided that the section's purpose was to ensure 'that a person cannot be prosecuted where, at the time of disclosure, it was not appropriate that the information had a security classification'.[108] The IGIS supported the inclusion of such a requirement, noting that section 50A operates as a condition precedent to the initiation of a prosecution and does not serve as prima facie evidence of that matter in the prosecution.[109]

3.124 The Attorney-General's Department did not initially support the inclusion of a requirement similar to section 50A of the *Australian Border Force Act*. The Department referred to the 'evidentiary certificates' provisions in the Bill (discussed below) and advised that it would be inappropriate to require the Attorney-General to issue an evidentiary certificate in every matter on the basis that 'this is not an objective fact but rather a statement of opinion, which would not properly belong in an evidentiary certificate'.[110] The Attorney-General's Department did not consider whether a certificate of the kind issued under section 50A of the *Australian Border Force Act* could be issued, rather than an evidentiary certificate.

3.125 The Inspector-General responded to the Attorney-General Department's advice as follows:

> I note the views expressed on section 50A of the [*Australian Border Force Act*] in the supplementary submission of the Attorney-General's Department. It was suggested that the accuracy or appropriateness of a classification at the time of the conduct constituting the offence is a matter of opinion that would be unsuitable for inclusion in an evidentiary certificate issued by the Attorney-General. A certificate of the kind specified in section 50A of the ABF Act is not

---

107 Law Council of Australia, *Submission 5*, p. 8.

108 Revised Explanatory Memorandum to the Australian Border Force Amendment (Protected Information) Bill 2017, p. 18

109 Inspector-General of Intelligence and Security, *Submission 13.1*, p. 8.

110 Attorney-General's Department, *Submission 6.1*, p. 3-5.

> an evidentiary certificate (in the sense of being prima facie evidence of a matter in a prosecution or any other proceedings). Rather, it is a condition precedent to the commencement of a prosecution. The reasons that a matter of opinion could not properly form the basis for such a condition are not readily apparent.

3.126 The Inspector-General noted that the *Australian Border Force Act* offence carries a maximum penalty of imprisonment for two years, considerably less than those offences proposed by the Bill. The Inspector-General noted that an unauthorised disclosure of 'security classified information' could potentially constitute an offence under both acts, however, the more serious offences in the Code would not contain an equivalent condition to the commencement of a prosecution to that applying to the less serious offence in the *Australian Border Force Act*.[111]

3.127 Following the Inspector-General's response, the Department indicated that it had 'noted' the Inspector-General's suggestion and discussed it with her.[112] The Department indicated that if such an amendment were to be made, it would, 'as a condition precedent to a prosecution', require 'somebody' to assess and certify that the classification was accurate:

> So somebody other than the originating agency would therefore have undertaken an assessment that, even if it was a historical document, for a prosecution to proceed, the classification of secret or top secret remained accurate at the time the offence was committed.[113]

Strict liability

3.128 As outlined above, a number of offences in the Bill require the prosecution to prove that the information or article in question possessed a security classification. For the majority of offences, the Bill proposes that strict liability will apply to these elements.

---

111 Inspector-General of Intelligence and Security, *Submission 13.2,* p. 9.

112 Ms Tara Inverarity, Assistant Secretary, Attorney-General's Department, *Committee Hansard*, Melbourne, 16 March 2018, p. 59.

113 Ms Tara Inverarity, Assistant Secretary, Attorney-General's Department, *Committee Hansard*, Melbourne, 16 March 2018, p. 59.

Table 3.1 Offences with a 'security classification' strict liability component

Provision	Offence	Strict liability provision
Espionage—dealing with information etc. concerning national security which is or will be made available to foreign principal - intention as to national security *Penalty: life imprisonment*	91.1(1)(b)(i)	91.1(3)
Espionage—dealing with information etc. concerning national security which is or will be made available to foreign principal - reckless as to national security *Penalty: imprisonment for 25 years*	91.1(2)(b)(i)	91.1(3)
Espionage—security classified information etc. *Penalty: imprisonment for 20 years*	91.3(c)(i)	91.3(3)
Aggravated espionage offence *Penalty: if the penalty for the underlying offence is 20 years – imprisonment for 25 years; if the penalty for the underlying offence is 25 years - imprisonment for life.*	91.6(1)(b)(iii)	91.6(3)
Inherently harmful information - Communication of inherently harmful information *Penalty: imprisonment for 15 years*	122.1(1)(b)	122.1(5)
Inherently harmful information - Other dealings with inherently harmful information *Penalty: imprisonment for 5 years*	122.1(2)(b)	122.1(5)
Inherently harmful information - Information removed from, or held outside, proper place	122.1(3)(b)	122.1(5)

of custody *Penalty: imprisonment for 5 years*		
Inherently harmful information - Failure to comply with direction regarding information *Penalty: imprisonment for 5 years*	122.1(4)(d)	122.1(5)
Aggravated offence (secrecy) *Penalty: adds five years to the penalty for the underlying offence*	122.3(1)(b)(iii)	122.3(3)

3.129 The effect of applying strict liability is that no fault element needs to be proved. For example, for an espionage offence, the prosecution will be required to prove that the information has a security classification but will not need to prove that the person who dealt with the information knew of or was reckless as to the classification.[114]

3.130 The only defence available to this element will be the defence of mistake of fact. This defence would require a defendant to prove that they actively turned their mind to the question of whether the information had a security classification (or a particular classification), but acted upon the mistaken, but reasonable belief, that the information did not have a security classification.[115]

3.131 A number of submitters opposed the application of strict liability in these circumstances.[116] Mr Paul Murphy, Chief Executive of the Media, Entertainment and Arts Alliance, described the imposition of strict liability upon journalists who receive documents as 'extraordinary and intolerable'.[117]

---

114 *Criminal Code*, section 6; Explanatory Memorandum, p. 16.

115 *Criminal Code*, section 6.1(1)(b) and section 9.2.

116 Law Council of Australia, *Submission 5*, p. 23; Joint Media Organisations, *Submission 9* p. 3; Human Rights Law Centre, *Submission 11*, p. 3; Australian Human Rights Commission, *Submission 17*, p. 4.

117 Mr Paul Murphy, Chief Executive, Media, Entertainment and Arts Alliance, *Committee Hansard*, Canberra, 16 February 2018, p. 29.

3.132 The Explanatory Memorandum recognises that the proposed imposition of strict liability upon these elements may limit the presumption of innocence. The Explanatory Memorandum states:

> The application of strict liability may limit the presumption of innocence to the extent that it allows for the imposition of criminal liability without requiring the prosecution to prove fault in the defendant for that particular element. Strict liability provisions will not violate the presumption of innocence so long as they are reasonable in the circumstances, and maintain rights of defence.[118]

3.133 The Explanatory Memorandum states that applying strict liability is appropriate because

> information or articles carrying a security classification are clearly marked with the security classification and any person who has access to security classified information should easily be able to identify as such.[119]

3.134 This explanation was repeated by the Attorney-General's Department, which advised:

> Given the security classifications are prominently marked on documents, it is unnecessary to require proof of the fact of the classification.[120]

3.135 In contrast, the Australian Human Rights Commission submitted:

> The fact that the material is classified may well be unknown (and unknowable) by the discloser – particularly if they are an 'outsider'. … Applying strict liability to a matter about which a person cannot inform themselves in advance does not allow the person to be aware of their obligations and to regulate their conduct accordingly.[121]

3.136 The Law Council of Australia raised concerns that a document may be altered by a person to remove the security classification, such that any subsequent person dealing with the altered document may not be aware that the classification had been removed.[122]

---

118 Explanatory Memorandum, p. 16.

119 Explanatory Memorandum, p. 108.

120 Attorney-General's Department, *Submission 6.2*, p. 2.

121 Australian Human Rights Commission, *Submission 17*, p. 4.

122 Law Council of Australia, *Submission 5*, p. 24.

3.137 The Department noted that the effect of removing strict liability would be that the prosecution would need to prove that the defendant was reckless as to whether the information or article had a security classification.[123]

Evidentiary certificates

3.138 Proposed sections 93.3 and 121.3 in the Bill provides that the Attorney-General may sign an evidentiary certificate for the purposes of espionage and secrecy proceedings. The certificates will operate as prima facie evidence that:

- the information or article in question has or had a security classification, or a specific security classification, at a certain point in time; or
- the information or article in question 'concerns' Australia's national security or concerns a particular aspect of Australia's national security (espionage proceedings only).[124]

3.139 The evidentiary certificate will create an evidentiary presumption, which the defendant will be required to disprove.[125] The Explanatory Memorandum states:

> Evidentiary certificates … will be used to settle formal matters of fact (that the information or article concerns national security or is security classified) which may otherwise be difficult to prove under the normal rules of evidence.
>
> This is because matters concerning Australia's national security and security classified information can be said to be peculiarly within the knowledge of the Commonwealth. Further, allowing evidentiary certificates to be issued will protect sensitive information and technical capabilities without having a detrimental effect of the defendant's right to a fair trial.[126]

3.140 As noted above, the Explanatory Memorandum states that 'information or articles carrying a security classification are clearly marked with the security classification and any person who has access to security classified

123 Attorney-General's Department, *Submission 6.1*, p. 17.

124 Proposed section 93.3.

125 Explanatory Memorandum, p. 205.

126 Explanatory Memorandum, p. 205.

information should easily be able to identify as such'.[127] However, the Explanatory Memorandum also states:

> The evidentiary certificate framework in new section 121.3 is intended to facilitate the settling the formal question of whether particular information has, or had [at] a particular time, a security classification or a specified level of security classification, in limited cases where a security classification is not clearly marked on a particular document or piece of information. This may include cases where, for example:
>
> - a person has communicated information orally, and that information is, or was at the relevant time, security classified
> - a person has modified a document to remove any labels denoting its security classification
> - a person has communicated an excerpt from a security classified document, and that excerpt does not include a label denoting a security classification
> - a person has removed security classified information from a database, and the form in which it was removed does not include a label denoting a security classification, or
> - the information or document contains paragraph markings that are an abbreviated or shorthand reference to a security classification.[128]

3.141 Several submitters raised concerns regarding the proposed introduction of evidentiary certificates, in particular, how these certificates would operate to reverse the burden of proof.[129]

3.142 The Explanatory Memorandum concedes that the provision of evidentiary certificates will limit the presumption of innocence.[130] Commenting on this concession, Australian Lawyers for Human Rights submitted that:

> … given the seriousness of the offences involved, [evidentiary certificates] are inconsistent with the principles that form the bedrock of Australia's criminal justice system as well as international human rights standards.[131]

---

127 Explanatory Memorandum, p. 108.

128 Explanatory Memorandum, pp. 234–235.

129 Australian Lawyers Alliance, *Submission 12*, pp. 12-13; Dr Lawrence McNamara, *Submission 19*, p. 2 (in relation to the proposed use of evidentiary certificates in s. 122.3). relating to the question of whether information had a security classification for the purposes of a prosecution for a secrecy offence.)

130 Proposed sections 91.1, 91.3, 91.6 (espionage offences), 122.1, 122.2, 122.3 (secrecy offences).

3.143 Similarly, the Australian Lawyers Alliance recommended that:

> Evidentiary certificates should not be available to allow prosecutors to avoid having to prove all elements of a crime. Where national security requires that evidence should not be presented in court, the court's discretion in how proceedings are run should be relied on.[132]

3.144 The Australian Lawyers Alliance submitted that, given the severity of applicable penalties, it is more appropriate for the Court to determine these matters.[133]

3.145 The Attorney-General's Department's *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* (the Guide) states that 'limits should be placed on the use of evidentiary certificate provisions':

> Evidentiary certificates should generally only be used to settle formal or technical matters of fact that would be difficult to prove by adducing admissible evidence. It is generally unacceptable to use evidentiary certificates to cover questions of law, which are for the courts to determine.[134]

3.146 The Explanatory Memorandum states:

> [I]t may be difficult to settle the question of whether the particular information has a security classification, or had a security classification at a particular time, by adducing admissible evidence. It would often be necessary to adduce the original document or information from which the information was drawn into evidence. The admission into evidence of additional security classified information may risk compounding the harm to essential public interests by providing the defendant with additional security classified information that they have no need to know, as well as risking the further exposure of that information.
>
> It would often be necessary to put in place additional controls to protect the security classified information, such as those available under the *National Security Information (Criminal and Civil Proceedings) Act 2004*, which may impose additional burdens on the prosecution, defendant and court. In cases where the question of whether the information is, or was at a particular time,

131 Australian Human Rights Law Centre, *Submission 11*, p. 3.

132 Australian Lawyers Alliance, *Submission 12,* p. 19.

133 Australian Lawyers Alliance, *Submission 12*, p. 13.

134 Attorney-General's Department, *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*, September 2011, pp. 54–55.

> security classified information is essentially formal in nature, the use of a prima facie evidentiary certificate would facilitate the settling of that question by avoiding the difficulty of adducing additional classified evidence and the resultant imposition of potentially burdensome obligations on the parties and court.[135]

3.147 As discussed above, a number of submitters raised concerns that national security information is routinely over-classified or incorrectly classified. In this context, the Centre for Media Transition raised concerns that the Bill empowers the Attorney-General to issue an evidentiary certificate 'without any requirement to actively consider whether the security classification was appropriate or whether the material might actually be harmful'.[136]

3.148 The Inspector-General similarly pointed to this issue:

> As a practical matter, it is very difficult to see how a person could mount an effective challenge to such a certificate, given that they may not have access to the information or thing that is the subject of the certificate, or to the documents incorporated into the definition of a 'security classification' by the regulations.[137]

3.149 Submitters raised concerns that the difficulties associated with the use of security classifications as the basis for criminality would be exacerbated by the proposed application of strict liability and evidentiary certificates.[138] For example, Dr Lawrence McNamara of the York Law School, University of York submitted:

> … strict liability offences, combined with an AG certificate, appears to mean that prosecution would be able to proceed very substantially on the basis of assertion by the state of the significance of information (which though only prima facie evidence would be difficult to contest—perhaps so difficult that fair trial and equality of arms concerns might be invoked), and without proof of damage.[139]

3.150 Dr McNamara submitted that these provisions could result in circumstances where:

---

135 Explanatory Memorandum, p. 205.

136 University of Technology Sydney, Centre for Media Transition, *Submission 23*, p. 4.

137 Inspector-General of Intelligence and Security, *Submission 13*, p. 8.

138 Law Council of Australia, *Submission 5*, p. 23; Human Rights Law Centre, *Submission 11*, p. 21.

139 Dr Lawrence McNamara, *Submission 19*, p. 2.

> … individuals are successfully prosecuted but without any transparency around what, exactly, the substance of the offence was and whether it really did pose any risk.[140]

Government proposed amendments

3.151 On 13 February 2018, the Attorney-General's Department advised the Committee that the Attorney-General had instructed the Department to progress a number of changes to the Bill. The Committee received draft amendments to this effect from the Attorney-General on 5 March 2018. The proposed amendments included amending the definition of 'security classification' in section 90.5 to mean a classification of TOP SECRET or SECRET, or any other equivalent classification or marking prescribed by the regulations. The Attorney-General explained:

> Consistent with the Australian Government's Information Security Management Guidelines (available at www.protectivesecurity.gov.au), information should be classified as TOP SECRET if the unauthorised release of the information could cause exceptionally grave damage to the national interest. Information should be classified as SECRET if the unauthorised release of the information could cause serious damage to the national interest, organisations or individuals.
>
> The new definition will not allow for lower protective markings to be prescribed in the regulations and will only allow equivalent classifications or markings to be prescribed. This will allow flexibility to ensure the definition can be kept up to date if new protective markings of equivalent seriousness are introduced, or to ensure information bearing former protective markings of equivalent seriousness can continue to be protected.[141]

3.152 The proposed amendments also remove the provisions that apply strict liability to the elements of the secrecy and espionage offences that rely on security classifications.[142] The Attorney-General explained:

> The effect of these amendments is that, in addition to proving that information or article had a security classification, the prosecution will also have to prove that the defendant was reckless as to the fact that the information or article had a security classification. Consistent with section 5.4 of the *Criminal*

---

140 Dr Lawrence McNamara, *Submission 19*, p. 2.

141 Attorney-General, *Submission 40*, p. 2.

142 Proposed sections 91.1(3); 91.3(3); 91.6(3); 122.1(5); and 122.3(3).

> *Code Act 1995*, this will require proof that the person was aware of a substantial risk that the information had a security classification and, having regard to the circumstances known to him or her, it was unjustified to take the risk.[143]

3.153 Supplementary submissions to the Committee generally expressed support for the proposed amendments, subject to certain continuing reservations.[144] The joint councils for civil liberties, for example, noted that the amendments were 'positive' but that they 'retain some uncertainty as to the robustness and reliability of the classification system even at this level'.[145]

3.154 The Human Rights Law Centre described the amendments as a 'definite improvement', but reiterated its concern that security classification is 'an administrative systems that is not suitable for inclusion as an element in a serious criminal offence'. The Centre recommended the following safeguards to be implemented in addition to the proposed amendments:

> (a) mandatory guidelines be set out, for instance, in regulations, for the use of these higher-level classifications, setting out the criteria to be met and the oversight applied to classification decisions,
>
> (b) a legislative requirement be introduced that the security classification be confirmed prior to the institution of any criminal proceedings,
>
> (c) procedures be instituted for timely declassification, and
>
> (d) measures be introduced to address the documented practice of over-classification.[146]

3.155 The IGIS noted that the terms SECRET and TOP SECRET would 'take their meaning *exclusively* from policy as in force from time-to-time'. The IGIS expressed her continued support for:

- further statutory parameters for the regulation-making power in proposed section 90.5,
- a legislative requirement that any material incorporated by reference into the regulations must be publicly available, and

---

143 Attorney-General, *Submission 40*, p. 4.

144 Law Council of Australia, *Submission 5.1*, pp. 2–3; Human Rights Law Centre, *Submission 11*, p. 3; Joint councils for civil liberties, *Submission 31.1*, p. 4.

145 Joint councils for civil liberties, *Submission 31.1*, p. 4.

146 Human Rights Law Centre, *Submission 11*, p. 3.

- a legislative requirement that a security classification within the meaning of section 90.5 must be a classification that is assigned for the purpose of protecting national security.[147]

Committee comment

3.156 As discussed in Chapter 1, the Committee has reviewed the Bill with a view to ensuring that each measure is clear and unambiguous in its terms; proportional and appropriately targeted to the threat; and enforceable.

3.157 The Committee supports the Attorney-General's proposal to amend the Bill to define 'security classification' to mean SECRET and TOP SECRET (or equivalent) classifications. These are the two highest levels of security classification, and denote that the official who created the information considers that its disclosure would cause serious or grave harm. The Committee notes the department's evidence that the classification of information at these levels, in particular, will often depend on contextual information that only the originating agency has access to. The Committee is regularly briefed on information classified at these levels and understands that the reasons for which a particular classification is applied may not always be obvious to a person who is not intimately familiar with the matter. Accordingly, the Committee accepts both that the unauthorised disclosure of highly classified information has the potential to cause very serious harm and that, in principle, a person who is aware of a substantial risk that they may be dealing with such information and who elects to disclose it irrespective of what harm may follow may properly be considered culpable. However, the Committee considers that a number of amendments are required to ensure that the use of security classifications as a basis for criminal liability results in a legal framework that is clear and unambiguous; proportionate and appropriately targeted; and enforceable.

3.158 The proposed amendments enable the secrecy and espionage offences in the Bill to be more narrowly targeted, and go some way to addressing concerns that the term 'security classification' is not defined and therefore lacks clarity. However, the Committee is of the view that for greater certainty, the Bill should both list the classifications to which liability attaches, and prescribe the characteristics and qualities of that security classification. Any

147 Inspector-General of Intelligence and Security, *Submission 13.2*, p. 8.

material incorporated by reference into the regulations should also be required to be publicly available.

3.159 The Committee also recognises submitters' concerns that the government's classification system is essentially administrative in nature. The Committee notes evidence suggesting a tendency for officers to err on the side of caution by 'over-classifying' information; and that correctly classified information may become incorrectly classified due to the passage of time. In those instances, the nexus between the information and harm to national security is not apparent.

3.160 The Committee also notes a number of practical matters concerning the enforceability of the standard 'has a security classification'. The Explanatory Memorandum and the Attorney-General's Department's submission indicate that information and articles will be clearly and/or prominently marked with their security classification, and so any person with access to the information will be aware of its classification.[148] For example, if a person removed a TOP SECRET report from their workplace, this would most likely be marked with its classification TOP SECRET in the header and footer of each page. If that person provided the primary document, or a full copy of it, to another person, that second person could easily identify what classification the document possessed. If the second person passed the primary document in full to a third person, this third person would be equally able to identify its classification.

3.161 However, not all information which could be the subject of a secrecy or espionage offence will be 'marked' with a security classification. The secrecy and espionage offences are not limited to original primary documents. 'Information' is defined to include information of any kind, whether true or false, whether in material form or not, and including an opinion or a report of a conversation.[149] An 'article' includes any thing, substance or material.[150] 'Dealing with information or an article' will be defined to include dealing

148 Explanatory Memorandum, pp. 16, 108, 112, 121, 131, 239, 242, 243,.246, 250, 269; Attorney-General's Department, *Submission 6.1,* pp. 13, 29; *Submission 6.2,* p. 2.

149 *Criminal Code*, section 90.1.

150 *Criminal Code*, section 90.1.

with part of the information or article; or the substance, effect or description of the information or article.[151]

3.162 An offence can therefore arise in circumstances where a person dealt with information in a non-documentary form, such as a conversation. Similarly, documents other than exact copies will also be captured, for example, a record of a conversation, a description of material, a part of a document, content copied and pasted from an original document into another form, or information appearing in a media article. In these circumstances it is either unlikely, or in some cases not possible for the information to be 'prominently marked' with a security classification. Given the broad spectrum of information and conduct captured by these provisions, the Committee supports the Attorney-General's proposal to remove strict liability from the relevant offences, which would have the effect of requiring the prosecution to prove beyond reasonable doubt that the person was aware of a substantial risk that the information had a security classification and that in all the circumstances it was unreasonable for the person to take that risk, and further considers that evidentiary certificates should be removed from the Bill.

3.163 Additionally, the Committee understands that a document's classification denotes the classification level of the most sensitive information contained in the document, or the classification of the sum total of the opinion and information expressed in the document.[152] The document may also contain a range of paragraphs, sentences, ideas, quotes, names and facts which are unclassified, publicly available or possess a lower classification level than that appearing in the header and footer of a document. Thus, a person describing the substance of a paragraph of a TOP SECRET document, may in fact only be referring to publicly available material. The same would be true of non-documentary forms of information. In these circumstances the harm caused could be negligible or non-existent. Similarly, there may be situations in which information warrants a SECRET or TOP SECRET classification at

---

151 Proposed sections 90.1(1) and 90.1(2). The Bill proposes that section 90.1(2) only applies to the espionage offences. However, the government amendments provided to the Committee on 5 March 2018 will extend the application of section 90.1(2) to the secrecy offences.

152 The *Information security management guidelines - Australian Government security classification system* provides that information derived directly from security classified sources is to carry, at a minimum, the highest security classification of any of its sources (at [30]).

the time it is authored, but loses that quality with the passage of time. In these circumstances, no damage would arise.

3.164 For these reasons, the Committee considers that, for offences relying on the security classified nature of a document or piece of information, safeguards should be implemented to ensure that it was appropriate for the particular classification to applied to that document or piece of information.

3.165 The Committee considers that the introduction of an administrative process to confirm the appropriateness of a classification prior to trial (akin to section 50A of the Border Force Act) is an important and necessary safeguard. This is particularly necessary in light of the serious penalties which are proposed (ranging up to life imprisonment) and other serious consequences which will flow from being charged with some secrecy or espionage offences, including being denied bail, minimum non-parole periods, deportation and citizenship loss (see Chapter 10). As noted above, the Committee appreciates that the reasons for which a document or piece of information was originally classified—and for which it should or should not remain classified—will often only be known by the originating agency. Where information is classified TOP SECRET, in particular, those reasons will often be exceptionally sensitive, going to the identities of delicate human sources or highly sensitive technical capabilities, and would often be known only to a limited range of people inside the relevant agency. Accordingly, the Committee considers that it is appropriate that the head of the originating agency should be required to certify the appropriateness of the classification.

3.166 The administrative process of confirming the appropriateness of the security classification should operate as a condition precedent to prosecution, rather than acting as prima facie evidence of the fact in question. To uphold the accused's right to a fair trial, the Crown should be required to prove that as at the time the alleged offence was committed:

- the information 'had a security classification'; and
- the accused knew or was reckless as to this; and
- at that time the information necessitated a SECRET or TOP SECRET security classification.

Recommendation 8

3.167 The Committee recommends that the Bill be amended to define each 'security classification' to which criminal liability attaches. Each

definition should include harm-based statutory criteria for determining the proper classification to apply to that information. Any material incorporated by reference into the regulations should be required to be publicly available.

Recommendation 9

3.168 The Committee recommends implementing the Attorney-General's proposed amendments to

- **narrow the proposed definition of 'security classification' to a classification of SECRET or TOP SECRET, or equivalent, and**
- **remove strict liability from espionage and secrecy offences.**

Recommendation 10

3.169 The Committee recommends that the Bill be amended to require that, prior to initiating proceedings for an espionage or secrecy offence that relies on the fact that information is security classified, the head of the originating agency must certify that it is appropriate that the information had a security classification at the time of the conduct that is alleged to constitute the offence.

This certificate should operate as a condition precedent to the initiation of proceedings. The certificate should not have any evidentiary effect.

Recommendation 11

3.170 The Committee recommends that the Bill be amended to remove the evidentiary certificate regimes in proposed sections 93.3(1)(a)-(b) and 121.3, in relation to security classified information.

Evidentiary certificates - 'concerns national security'

3.171 Proposed section 93.3 would enable the Attorney-General to issue an evidentiary certificate for espionage proceedings, which will be prima facie evidence that the information or article in question 'concerns Australia's

national security' or concerns a particular aspect of Australia's national security.[153]

3.172 In addition to the general arguments against evidentiary certificates, discussed above, submitters also raised specific concerns regarding the availability of an evidentiary certificate to provide prima facie evidence that a matter 'concerns' national security. The Australian Lawyers Alliance submitted:

> … if an evidentiary certificate were issued by the Attorney-General to say that a particular matter is related to national security, it would then be up to the defendant to disprove that contention. This places an impossible burden on defendants. … While the Explanatory Memorandum states that the use of evidentiary certificates will not have 'a detrimental effect on the defendant's right to a fair trial', the ALA questions how such an effect could be avoided …
>
> Given the severe penalties that stem from an item being found to concern Australia's national security, we believe that it is more appropriate for a court, rather than the Attorney-General, to be empowered to rule on this matter.[154]

3.173 The Law Council of Australia noted that proposed section 93.3 would 'give discretion to the Attorney-General as to when to certify information or an article' and would 'in effect allow information or a thing to be certified after the time of the conduct that is alleged to constitute the offence':

> That is, an element of retrospectivity would potentially occur in relation to the espionage and foreign interference offence provisions. The Law Council considers that a prosecution should not be initiated unless it has been certified that it is appropriate that the information concerned Australia's national security (or Part thereof) at the time of the conduct that is alleged to constitute the offence. This would limit potential for retrospective application.[155]

3.174 In response to this concern, the Attorney-General's Department submitted:

> The department does not agree the Attorney-General should certify that it was 'appropriate' for the information to 'concern national security' at the time of the conduct constituting the offence. This is not an objective fact but rather a statement of opinion, which would not properly belong in an evidentiary certificate. The *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* states that evidentiary certificates are generally only

153 Schedule 1, item 20 (proposed section 93.3 of the *Criminal Code*)

154 Australian Lawyers Alliance, *Submission 12*, p. 13.

155 Law Council of Australia, *Submission 5*, p. 19.

> suitable when they relate to formal or technical matters of fact that would be difficult to prove by adducing admissible evidence.[156]

3.175 The Law Council also submitted that it was unclear whether there was scope in proposed subsection 93.3(1) for the Attorney-General to 'expand the meaning of "national security" beyond the confines of the proposed statutory definition'. It recommended that the subsection be amended 'to require the Attorney-General to only certify information or an article as concerning Australia's national security subject to the statutory criteria for "national security"'.[157]

3.176 The Attorney-General's Department responded:

> The Bill already achieves this effect. The definition of 'national security' will be inserted into Division 90, which sets out the definitions for Part 5.2 of the Criminal Code. Section 93.3 will be located in Part 5.2. Therefore, for the purposes of section 93.3, the Attorney-General will only be able to certify that information concerns 'national security' within the definition of the term in section 90.4.[158]

Committee Comment

3.177 The Committee does not consider that the use of evidentiary certificates is appropriate in these circumstances. The Committee considers that the question of whether a matter 'concerns' national security may be contestable, and is therefore not a 'formal or technical matter of fact' that is appropriate to include in an evidentiary certificate. Accordingly, the Committee recommends removing these provisions from the Bill.

Recommendation 12

3.178 The Committee recommends that the Bill be amended to remove the evidentiary certificate regimes in proposed sections 93.3(1)(c)-(d), in relation to information that 'concerns Australia's national security'.

---

156 Attorney-General's Department, *Submission 6.1*, p. 3.

157 Law Council of Australia, *Submission 5*, pp. 19–20.

158 Attorney-General's Department, *Submission 6.1*, p. 3.

Preparatory offences

3.179 Several of the proposed offences in the Bill criminalise preparatory conduct. These are:

- 82.9 – Preparing for or planning sabotage offence,
- 91.12 – Offence of preparing for an espionage offence, and
- 92.4 – Offence of preparing for a foreign interference offence.

3.180 Some submitters were of the view that the preparatory offences were not required, given the availability of the offence of attempt, which would ordinarily apply under section 11.1 of the Criminal Code.[159]

3.181 Sections 11.1, 11.4 and 11.5 of the *Criminal Code* outline existing offences for

- **attempt**—a person who attempts to commit an offence commits the offence of attempting to commit that offence and is punishable as if the offence attempted had been committed,
- **incitement**—a person who urges the commission of an offence commits the offence of incitement, and
- **conspiracy**—a person who conspires with another person to commit an offence punishable by imprisonment for more than 12 months commits the offence of conspiracy to commit that offence is punishable as if the offence to which the conspiracy relates had been committed.

3.182 The Australian Lawyers Alliance objected to the introduction of the Bill's preparatory offences on the basis that

> this change would dramatically expand the preliminary activities that would be criminalised, including circumstances in which the accused could reasonably change their mind before the offence was committed.[160]

3.183 The Law Council raised a general concern around 'the increasing number of preparatory offences that are being introduced into the *Criminal Code*'. Since 2002, preparatory offences have been introduced in relation to terrorism and child sex offences.[161]

---

159 Law Council of Australia, *Submission 5*, p. 48; Australian Lawyers Alliance, *Submission 12*, p. 11-12.

160 Australian Lawyers Alliance, *Submission 12*, p. 11-12.

161 Law Council of Australia, *Submission 5*, p. 35. The Law Council refers to the Anti-Terrorism Bill (No 2) 2004; however, the offence of 'Other acts done in preparation for, or planning, terrorist

3.184 The Law Council suggested that, if the Committee does not agree that incitement, conspiracy and attempt provisions in Part 2.4 of the *Criminal Code* are sufficient to deal with preparatory conduct:

> [T]he Law Council recommends that there be a public review conducted by the Attorney-General's Department which clearly identifies the appropriate criteria which should be used for determining the kinds of criminal conduct that warrant preparatory offences. The review should allow for a public submissions process and the outcomes be used to inform the [*Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*].[162]

3.185 The Law Council contrasted the introduction of preparatory offences to the process undertaken in developing the *Criminal Code*:

> The committee met and prepared discussion papers on specific topics which eventually became chapters of the Criminal Code. The first one that was done was the principles of criminal responsibility, and then we went through various other things … That then was put out by way of discussion papers, and the committee did road shows all over the country, talking to all sorts of vested and non-vested interests about the proposals. Those proposals were then revised, and we ultimately then would provide a report in each of these areas. We submitted that to the government, it went through the processes and in 1995 the legislation was passed. That to me was a model of careful policymaking. The detailed consultation process and discussions with public defenders offices, DPPs, police, victims groups and so on made enormous improvements in refining that body of work.[163]

3.186 The Law Council argued that the preparatory offences proposed in the Bill 'really need to be carefully thought through and not to deal with such broad and vague concepts':

> I remember that in the course of discussions of terrorism legislation with Senator Brandis there was discussion of why there is a need for a preparation offence. Why not attempt or conspiracy? He said, 'Look, that's only meant to capture the lone wolf attack.' The act of preparation was meant for lone wolves. I had the misfortune some years later to be doing an appeal involving five accused charged with conspiring to do an act of preparation, and that was

---

acts' in section 101.6 of the *Criminal Code 1995* was inserted by the *Security Legislation Amendment (Terrorism) Act 2002*.

162 Law Council of Australia, *Submission 5*, p. 35.

163 Dr David Neal, SC, Member, National Criminal Law Commission, Law Council of Australia, *Committee Hansard*, Melbourne, 16 March 2018, pp. 10–11.

> the case where we had a 500-page charge to the jury, because conspiracy and the act of preparation are really complicated things. In the context of multiple trials, it's just making trouble.[164]

3.187 The Attorney-General's Department disagreed with the Law Council that that the extensions of criminal responsibility in Part 2.4 are sufficient, and noted that preparatory offences are generally reserved for serious criminal conduct warranting criminalisation at the preparation stage:

> This offence will give law enforcement authorities the means to deal with preparatory conduct, without the need to, for example, wait until a foreign interference offence is committed or an Australian process is put at risk of interference.
>
> Liability for attempt arises from conduct that is 'more than merely preparatory' (subsection 11.1(2) of the Criminal Code). The proposed offence targets conduct that occurs before liability for attempt would arise. The preparatory offence criminalises conduct that would not yet amount to an attempt to commit a sabotage offence.[165]

3.188 The Department added:

> The *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* provides general guidance on the matters to be considered when developing or amending criminal offences and enforcement powers. The Guide does not reflect a binding policy position but provides principles and precedents to assist the framing of criminal offences and related matters. The Guide draws its principles and precedents from Senate Committees and other sources, such as the Australian Law Reform Commission. Should the Committees express particular views regarding preparatory offences, consideration would be given to including guidance on these as well.[166]

3.189 The Attorney-General's Department noted that the preparatory offences in the Bill are similar to those adopted in relation to terrorism and child sex offences,[167] and argued that

---

164 Dr David Neal, SC, Member, National Criminal Law Commission, Law Council of Australia, *Committee Hansard*, Melbourne, 16 March 2018, p. 11.

165 Attorney-General's Department, *Submission 6.1*, p. 15

166 Attorney-General's Department, *Submission 6.1*, p. 9.

167 Attorney-General's Department, *Submission 6*, p. 18. See sections 101.6, 272.20 and 474.25C of the *Criminal Code*.

> preparatory offences, although newer, are not unknown to the statute books and have been used in terrorism offences and in offences in relation to online harm against children. So we have, where appropriate, adopted and built on existing concepts which are known to the Commonwealth Criminal Code. Again, there is that body of jurisprudence and knowledge around the operation of the Commonwealth Criminal Code.[168]

Committee comment

3.190 The Committee notes that the *Criminal Code* already contains offences for incitement, conspiracy and attempt. The proposed preparatory offences in the Bill will extend beyond these concepts to the point of preparation or planning of a sabotage, espionage or foreign interference offence. The Committee will consider the appropriateness of these specific offences later in this report.

3.191 While the Committee notes that preparatory offences already exist in the *Criminal Code* in relation to terrorism and child sex offences, there does not appear to be any underlying principles or guidance as to the circumstances in which preparatory offences are justified. It is beyond the scope of this inquiry, or the functions of this Committee, to consider the appropriate role for preparatory offences in Commonwealth criminal law. However, to the extent that preparatory offences are used more commonly in relation to terrorism and, as proposed in this Bill, espionage and foreign interference, than in other parts of the statute book, it would assist the Committee if there were greater public guidance on this matter. Accordingly, the Committee recommends that the Government amend the *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* to identify criteria to be used for determining the kinds of criminal conduct that warrant preparatory offences.

Recommendation 13

3.192 The Committee recommends that the Government amend the *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* to identify criteria to be used for determining the kinds of criminal conduct that warrant preparatory offences.

---

168 Ms Anna Harmer, First Assistant Secretary, Attorney-General's Department, *Committee Hansard*, Melbourne, 16 March 2018, p. 40.

Reckless conduct

3.193 The Committee received evidence expressing a general concern with the number of offences in the Bill that have a fault element of recklessness rather than intent.

3.194 Section 5.4 of the *Criminal Code* provides that a person is reckless with respect to:

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

3.195 The *Criminal Code* provides that the question whether taking a risk is unjustifiable is one of fact. If recklessness is a fault element for a physical element of an offence, proof of intention, knowledge or recklessness will satisfy that fault element.

3.196 Australian Lawyers for Human Rights voiced its concern that

> the Bill continues this government's concerning and very undesirable pattern of criminalising 'reckless' behaviour that is in no way intended to cause harm, and quite irrespective of whether or not harm has actually been caused.[169]

3.197 In its submission, Human Rights Watch recommend removing reckless as a level of culpability.[170] The Australian Lawyers Alliance, in discussing espionage offences, saw the inclusion of the mental element of recklessness coupled with broader physical elements such as 'receiving, collecting or possessing information or an article' as a 'cause for concern'.[171]

3.198 The Attorney-General's Department explained that

> the effect of section 5.6 of the *Criminal Code* is that recklessness is the fault element if a physical element that is a circumstance does not specify a fault element … This is consistent with the *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement powers*, which states (at paragraph 2.2.4 on

169 Australian Lawyers for Human Rights, *Submission 7*, p.4.

170 Human Rights Watch, *Submission 10*, p. 2.

171 Australian Lawyers Alliance, *Submission 12*, p. 10.

> page 20) that the default elements supplied by section 5.6 of the *Criminal Code* should apply unless there is a sound reason to depart from them.[172]

3.199 The Attorney-General's Department explained the purpose of including recklessness elements in the espionage offences as follows:

> 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.[173]

Committee comment

3.200 The Committee notes that recklessness applies as the default mental element to many of the physical elements of the espionage offences, consistent with section 5.6 of the *Criminal Code* and the policy position set out in the *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement powers*. Where recklessness is included as a specific mental element, in subsections 91.1(2), 91.2(2) and 91.8(2), it attaches to physical elements that are results or circumstances. As noted above, recklessness is the default mental element for a physical element that is a circumstance. Similarly, recklessness is also the default mental element for a physical element that is a result. Accordingly, these offences do not appear to depart from the default approach to mental elements in the *Criminal Code* or for Commonwealth criminal law policy as set out in the Guide. Instead, these offences appear to exist as part of a tiered framework of offences—subsections 91.1(1), 91.2(1) and 91.8(1) contain offences attracting higher maximum penalties that require the prosecution to prove beyond reasonable doubt that the person intends a particular result, which is a higher threshold than is ordinarily required to establish criminal liability under the Code.

Evidential burden on the defendant

3.201 Many of the Bill's proposed new offences—including in relation to secrecy, espionage, foreign interference and sabotage—provide defences for

---

172 Attorney-General's Department, *Submission 6.3*, p. 3.

173 Attorney-General's Department, *Submission 6*, p. 15.

legitimate conduct, rather than excluding this conduct in the elements of the offence.

3.202 A number of submitters on the Bill expressed concerns about the offence-specific defences 'that reverse the burden of proof by providing that a defendant bears the evidential burden in proving the elements of the defence'.[174] For example, the IGIS noted the possibility that such a reversal of the onus of proof may deter individuals from bringing information to the IGIS's attention:

> As a general observation, it is possible that the prospect of exposure to criminal investigation and prosecution, and the need to satisfy a court of the evidential burden in relation to a defence, may deter some individuals from speaking up about real or perceived wrongdoing by an intelligence agency.[175]

3.203 The IGIS also pointed out that the 'interaction of section 34 of the *IGIS Act* and the proposed offences and defences in the Bill may have been overlooked'. The IGIS explained that, whilst the Explanatory Memorandum states

> in relation to the defence in proposed s 122.5(1), that 'the imposition of the evidential burden on the defendant is appropriate because the defendant should be readily able to point to evidence that their conduct was … done in their official capacity as a Commonwealth official'

the Explanatory Memorandum

> does not appear to acknowledge the possibility that a Commonwealth official may be subject to secrecy obligations under other laws, such as s 34 of the *IGIS Act*, which could prevent them from adducing the evidence that is necessary to discharge the evidential burden.[176]

3.204 The Australian Lawyers for Human Rights noted confirmation by the Explanatory Memorandum that the Bill does limit the presumption of innocence and that such limitation includes the reversal of the onus of proof by providing that a defendant bears the evidential burden in proving the elements of the defence:

> The Explanatory Memorandum concedes (par 69) that the Bill limits the presumption of innocence by:

---

174 Explanatory Memorandum, p. 18.

175 Inspector General of Intelligence and Security, *Submission 13*, p. 3.

176 Inspector General of Intelligence and Security, *Submission 13*, p. 6.

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

ALHR opposes these provisions which, given the seriousness of the offences involved, are inconsistent with the principles that form the bedrock of Australia's criminal justice system as well as international human rights standards.[177]

3.205 In relation to the secrecy of information offences in Schedule 2 to the Bill, the Australian Lawyers Alliance criticised the reliance on a defence of 'previously communicated information' at proposed section 122.5(8):

> This is an extraordinarily high bar for a defendant to reach in seeking to defend their actions. Usually, it would be expected that the prosecution would be required to show that the communication would cause harm, or there was reason to believe that harm would be caused. In this Bill, however, the onus is shifted to the defendant to show that (a) they had considered whether harm would come to Australia's interests; (b) they had come to the view that no harm would arise; and (c) this view was reasonable.
>
> This reversal of the onus of proof effectively shifts too much of the prosecutor's role of proving a crime beyond a reasonable doubt on to the defendant. The ALA believes that, rather than requiring defendants to show that they had considered the impact of a communication on Australia's interests, security or defence, it must be up to the prosecution to show that the defendant had intended to cause harm.[178]

3.206 In contrast, the Law Council of Australia's submission was critical of the certain defences proposed to be available to public officials. It stated that:

> a person acting in their capacity as a public official should not be permitted to act with the intention of, or be reckless as to, prejudicing Australia's national security. Such a defence for public officials appears antithetical to the very intent of the Bill, namely, to protect Australia against acts of sabotage, espionage and foreign interference. Furthermore, such a defence would in practice be unnecessary in circumstances where a court may consider that the

---

177 Australian Lawyers for Human Rights, *Submission 7*, p. 3. (emphasis added)

178 Australian Lawyers Alliance, *Submission 12*, p. 17.

requisite fault elements once proven by the prosecution are inconsistent with a public official acting in their capacity.

This difficulty does not arise for those offences where it may reasonably be envisaged that a public official may be requested to engage in certain conduct such as intending to advantage the national security of a foreign country (such as an ally).[179]

3.207 The Attorney-General's Department's *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers* (the Guide) states that:

> It is a fundamental and long-standing principle of criminal law that a defendant is presumed to be innocent until proven guilty, and that the prosecution must prove every element of an offence beyond a reasonable doubt.[180]

3.208 The Guide states that:

> Offence-specific defences reverse the fundamental principle of criminal law that the prosecution must prove every element of the offence. Therefore, a matter should only be included in an offence-specific defence, as opposed to being specified as an element of the offence, where:
>
> - it is peculiarly within the knowledge of the defendant, and
> - it would be significantly more difficult and costly for the prosecution to disprove than for the defendant to establish the matter.[181]

3.209 The Guide further explains:

> The fact that it is difficult for the prosecution to prove a particular matter has not traditionally been considered in itself to be a sound justification for placing the burden of proof on a defendant. If an element of the offence is difficult for the prosecution to prove, imposing a burden of proof on the defendant in respect of that element may place the defendant in a position in which he or she would also find it difficult to produce the information needed to avoid conviction. This would generally be unjust. However, where a matter is

---

179 Law Council of Australia, *Submission 5*, p. 26.

180 Attorney-General's Department, *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*, September 2011, p. 50.

181 Attorney-General's Department, *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*, September 2011, p. 50.

> peculiarly within the defendant's knowledge and not available to the prosecution, it may be legitimate to cast the matter as a defence.[182]

3.210 In addition the Guide states that creating a defence is also more readily justified if:

- the matter in question is not central to the question of culpability for the offence,
- the offence carries a relatively low penalty, or
- the conduct proscribed by the offence poses a grave danger to public health or safety.[183]

3.211 The Australian Law Reform Commission's 2009 report, *Secrecy Laws and Open Government in Australia*, considered which exemptions and defences should be explicitly included in a general secrecy offence. The report drew a distinction between an 'exception', which limits the scope of conduct prohibited by a secrecy offence, and a 'defence', which may be relied on to excuse conduct that is prohibited by a secrecy offence.[184] The report concluded:

> In the ALRC's view, it is essential to include an exception in the general secrecy offence for disclosure in the course of an officer's functions or duties.[185]

3.212 The ALRC's 2016 report, *Traditional Rights and Freedoms—Encroachments by Commonwealth Laws*, notes the *Criminal Code* distinction between a 'legal burden'—which is the burden of proving the existence of a matter—and an 'evidential burden'—which is the burden of adducing or pointing to evidence that suggests a reasonable possibility that the matter exists or does not exist.[186] Although the Commission focused its inquiry on laws that reverse the legal burden of proof, it cited concerns expressed by some

---

182 Attorney-General's Department, *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*, September 2011, p. 50.

183 Attorney-General's Department, *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*, September 2011, p. 50.

184 Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, December 2009, pp. 228.

185 Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, December 2009, pp. 234.

186 Australian Law Reform Commission, *Traditional Rights and Freedoms—Encroachments by Commonwealth Laws*, December 2015, p. 261.

submitters about the reversal of the evidential burden, 'especially where the reversal applies to a key culpability element of a serious criminal offence'.[187]

3.213 The Explanatory Memorandum to the Bill discusses the reasonableness and proportionality of placing the burden of proof on the defendant:

> It is reasonable and necessary for the burden of proof to be placed on the defendant where the facts in relation to the defence are peculiarly within the knowledge of the defendant. For example, for a defence at section 91.4(2) (espionage) a defendant should be readily able to point to evidence that they acquired the relevant information or article indirectly from a publically available source. For a defence at subsection 83.3(2) (military-style training involving foreign government principal) the defendant is best placed to know of the existence of the type of agreement therein and to provide evidence in relation to that agreement. Similarly, for a defence at section 80.3 the defendant is best placed to explain their motivations when engaging in the relevant conduct as it is peculiarly within their knowledge as to how and why they should be considered to be acting in good faith.
>
> Reversal of proof provisions are proportionate … as the prosecution will still be required to prove each element of the offence beyond reasonable doubt. Further, if the defendant discharges an evidential burden, the prosecution will also be required to disprove those matters beyond reasonable doubt, consistent with section 13.1 of the Criminal Code.[188]

3.214 The Department explained its position on the reversal of the onus of proof as follows:

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

---

187 Australian Law Reform Commission, *Traditional Rights and Freedoms—Encroachments by Commonwealth Laws*, December 2015, pp. 262–263.

188 Explanatory Memorandum, pp. 18–19.

> It is also noted that in practice, the prosecution will have regard to any lines of defence which are plainly open on the evidence or have been indicated by an alleged accused when making a determination that there are reasonable prospects of conviction and that the matter should proceed.[189]

Rights to freedom of expression and political communication

3.215 A number of submitters on the Bill expressed their concern that the offences in the Bill may impinge on rights to freedom of expression and political communication.

3.216 The right to freedom of expression is enshrined in article 19 of the ICCPR, which provides:

> 1. Everyone shall have the right to hold opinions without interference.
>
> 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
>
> 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
>
> a. For respect of the rights or reputations of others;
>
> b. For the protection of national security or of public order (ordre public), or of public health or morals.[190]

3.217 In relation to laws for the protection of national security, a joint submission by three United Nations Special Rapporteurs stated that

> national security considerations should be 'limited in application to situations in which the interest of the whole nation is at stake, which would thereby exclude restrictions in the sole interest of a Government, regime, or power group.' Additionally, States should 'demonstrate the risk that specific expression poses to a definite interest in national security or public order, that

189 Attorney-General's Department, *Submission 6.1*, p. 52.

190 UN Human Rights Committee, *International Covenant on Civil and Political Rights*, article 19: Freedoms of opinion and expression.

> the measure chosen complies with necessity and proportionality and is the least restrictive means to protect the interest, and that any restriction is subject to independent oversight.'[191]

3.218 The Australian Human Rights Commission, whilst acknowledging the 'legitimacy of the Bill's overarching objective' considered that

> this objective could be achieved without impinging so significantly on human rights. Specifically, the Commission is concerned that the secrecy provisions in the Bill may limit the right to freedom of expression to a degree that has not been demonstrated to be necessary and proportionate to a legitimate objective.[192]

3.219 The Australian Constitution does not explicitly protect freedom of expression. However, the High Court has held that an implied freedom of political communication exists as an indispensable part of the system of representative and responsible government created by the Constitution. It operates as a freedom from government restraint, rather than a right conferred directly on individuals.[193] This was recently reaffirmed by the High Court in the decision *Brown v State of Tasmania:*

> The implied freedom protects the free expression of political opinion, including peaceful protest, which is indispensable to the exercise of political sovereignty by the people of the Commonwealth. It operates as a limit on the exercise of legislative power to impede that freedom of expression.[194]

3.220 Noting the lack of an explicit protection for freedom of expression the Australian Lawyers Alliance raised a concern that the Bill, as drafted, could be found by the High Court to impinge on the implied freedom of political communication:

> It is entirely possible that the court would find that the provisions contained in this Bill that relate to inhibiting communication or dealing with information conflict with the freedom of political communication. However, for such a

---

191 UN Special Rapporteurs, *Submission 30*, p. 4.

192 Australian Human Rights Commission, *Submission 17*, p. 1.

193 In *Nationwide News Pty Ltd v Wills* (1992) 177 CLR 1 and *Australian Capital Television Pty Ltd v the Commonwealth* (1992) 177 CLR 106, the majority of the High Court held that an implied freedom of political communication exists as an incident of the system of representative government established by the Constitution. This was reaffirmed in *Unions NSW v New South Wales* [2013] HCA 58.

194 *Brown v State of Tasmania* [2017] HCA 43 at [88].

> finding to be made, a challenge would be required. Establishing standing in constitutional cases can be complicated and, as far as the ALA is aware, is yet to be explored by the High Court with respect to counter-terrorism and other security-related matters. To this end, the Australian Law Reform Commission has noted the risk posed to freedom of expression by counter-terrorism legislation, and has recommended a review of such laws be conducted. As such, it is entirely possible that, if enacted, the reforms contained in this Bill may conflict with constitutional requirements, but continue to have a chilling effect on communications in the absence of any challenge.[195]

3.221 The Law Council states that:

> Laws that engage the freedom of expression must be necessary and proportionate to the protection of specific public interests. The proposed secrecy provisions in the Bill, due to their breadth, are arguably inconsistent with article 19 of the ICCPR and not in accordance with Australia's international obligations. They may also arguably be invalid on the basis that they infringe the constitutional protection of freedom of political communication.[196]

3.222 The Law Council urged the Committee to

> await the [Parliamentary Joint Committee on Human Rights (PJCHR)'s] assessment of the Bill for its impact on freedom of speech before completing its inquiry and if necessary, extend the opportunity to make submissions in response to the information obtained. Any issues identified by the PJCHR should be addressed prior to enactment.[197]

3.223 The Department addressed this suggestion as follows:

> The department has no comment to make on the timing of the Committee's inquiry. The department is happy to consider any issues raised by PJCHR in its consideration of the Bill.[198]

3.224 The Parliamentary Joint Committee on Human Rights' report *Human rights scrutiny report; Report 2 of 2018* examined the Bill and raised many issues in relation to the following rights:

---

195 Australian Lawyers Alliance, *Submission 12*, p. 18.

196 Law Council of Australia, *Submission 5*, pp. 55–56.

197 Law Council of Australia, *Submission 5*, p. 56.

198 Attorney-General's Department, *Submission 6.1*, p. 2.

- freedom of expression;
- right to an effective remedy;
- privacy; freedom of association;
- presumption of innocence;
- right to take Part in public affairs.[199]

3.225 The PJCHR have listed the Bill as requiring a response.[200]

3.226 In addition to areas where the offences in the Bill may limit the right to freedom of expression, the Explanatory Memorandum states:

> The Bill protects and promotes the right to opinion and freedom of expression, the freedom of assembly and association and the right to take part in public affairs and elections by:
>
> - introducing foreign interference offences, which will criminalise certain conduct that seeks to influence the exercise of Australian democratic or political rights, and
> - replacing the offence of 'interference with political liberty' with the offence of 'interference with political rights and duties'.[201]

---

199 Parliamentary Joint Committee on Human Rights: *Human rights scrutiny report; Report 2 of 2018*, 13 February 2018, p. 2.

200 The PJCHR list their conclusions on Bills as 'no concerns', 'advice only' or 'response required'.

201 Explanatory Memorandum, p. 8.

4. Secrecy offences - breadth of conduct captured

4.1 This chapter, and the following chapter, discuss the proposed new secrecy offences in Schedule 2 to the Bill.

4.2 The proposed secrecy offences were a topic of focus for many participants in the Committee's inquiry, with concerns centring on the breadth of conduct captured by the offences and limitations in the available defences. In response to these concerns, the Attorney-General proposed a number of amendments to the provisions during the course of the inquiry. The chapters consider the secrecy offences both as outlined in the Bill, and taking into account the Attorney-General's proposed amendments.

4.3 This chapter contains an overview of the provisions and considers

- the rationale for the proposed new offences,
- evidence received in relation to the Australian Law Reform Commission (ALRC)'s 2009 report, *Secrecy Laws and Open Government in Australia*,
- evidence concerning the breadth of conduct captured by the offences, and
- the Committee's conclusions in relation to these matters.

Overview of the provisions

4.4 The Bill repeals the existing general secrecy offences in sections 70 and 79 of the *Crimes Act 1914* (the Crimes Act) and replaces them with nine new underlying offences in new Part 5.6 of the *Criminal Code*:

Table 4.1 Secrecy offences

Offence	Clause	Penalty[1]
Inherently harmful information – communicating	122.1(1)	15 years
Inherently harmful information – other dealings	122.1(2)	5 years
Inherently harmful information – removed from/held outside proper place of custody	122.1(3)	5 years
Inherently harmful information – failing to comply with direction	122.1(4)	5 years
Conduct causing harm to Australia's interests – communicating	122.2(1)	15 years
Conduct causing harm to Australia's interests – other dealings	122.2(2)	5 years
Conduct causing harm to Australia's interests – removed from/held outside proper place of custody	122.2(3)	5 years
Conduct causing harm to Australia's interests – failing to comply with direction	122.2(4)	5 years
Unauthorised disclosure of information by Commonwealth officers and former Commonwealth officers	122.4(1)	2 years

4.5 The Bill also provides for aggravated offences carrying an additional five years penalty for each of the above 'inherently harmful information' and 'conduct causing harm' offences when any of the following circumstances apply:

- the information is classified SECRET or above;
- the offences involves five or more records with a security classification;
- the person alters the document to conceal or remove its security classification;
- the record is marked 'for Australian eyes only' or has another marking prescribed by the regulations; or
- at the time of the offence, the person held a security clearance.[2]

[1] The maximum penalties under the existing secrecy offences in the Crimes Act ranged from 6 months to 7 years imprisonment.

4.6 The secrecy offences are limited to information that was made or obtained by a person by reason of his or her being, of having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity. Information is defined in existing section 90.1 of the *Criminal Code* to mean information of any kind, whether true or false and whether in a material form or not, and includes an opinion and a report of a conversation.

4.7 The offences, however, will apply to conduct engaged in by any person, and is not limited to current or former Commonwealth officers.

4.8 There are no exceptions contained in the physical elements of the offences. However, offence-specific defences are available in certain circumstances, with the defendant bearing the evidential burden:

Table 4.2 Defences available

Defence	Communication	Other dealings	Proper place of custody	Lawful direction
Commonwealth officer exercising a power; or performing a function or duty (s. 122.5(1))	Yes	Yes	Yes	Yes
Dealings with information in accordance with an agreement or arrangement with the Commonwealth (s. 122.5(1))	Yes	Yes	Yes	Yes
Information has already been made public with the consent of the Commonwealth (s. 122.5(2))	Yes	Yes	Yes	Yes
Communications concerning the Inspector-General of Intelligence and Security, Commonwealth Ombudsman, Law Enforcement Integrity Commissioner and their staff (s. 122.5(3))	Yes	No	No	No
Public interest disclosures (s. 122.5(4))	Yes	No	No	No

[2] Proposed section 122.3. In effect, there being five aggravated offences for each underlying secrecy offence in proposed sections 122.1 and 122.2 creates a total of 41 secrecy offences in the Bill.

Communicating the information to a court or tribunal (s. 122.5(5))	Yes	No	No	No
The person is a journalist, the dealings were for the purposes of fair and accurate reporting, and in the public interest (s. 122.5(6)-(7))	Yes	Yes	Yes	No
Prior publication: the information has already been communicated, or made available to the public and the person communicating the information reasonably believes their communication will not cause harm to Australia's interests, security or defence (s. 122.5(8)).	Yes	No	No	No
Information relating to a person in certain circumstances (s. 122.5(9))	Yes	Yes	Yes	No

Rationale for the proposed new offences

4.9 The Attorney-General's Department submitted that 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.[3]

4.10 The Department noted that there had been calls for significant reforms to the general secrecy offences in the Crimes Act for 'many years', and that 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

[3] Attorney-General's Department, *Submission 6*, p. 24.

> 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.
>
> 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 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.[4]

4.11 The Department also noted that the existing secrecy provisions in the *Criminal Code* were enacted in their current form in 1960, with only minor amendments made since then. It highlighted the following deficiencies:

> 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.
>
> 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.[5]

4.12 While supporting the repeal of the existing offences, the Human Rights Law Centre questioned whether it was appropriate for the reformed secrecy offences to be included in a Bill focusing on espionage and foreign interference.[6] At a public hearing, Dr Aruna Sathanapally told the Committee that

---

4 Attorney-General's Department, *Submission 6*, pp. 25–26.

5 Attorney-General's Department, *Submission 6*, p. 30.

6 Human Rights Law Centre, *Submission 11*, p. 23.

> schedule 2 extends well beyond information emerging from intelligence agencies, or information concerning national security, to information about and held by all types of government agencies.[7]
>
> … By contrast to the case for repealing sections 70 and 79, which is well known and has been called for for a very long time, the need for this specific legislation and the breadth of it is something that, to some extent, has come as a surprise for those of us who have been following secrecy offences. It's not clear to us why these offences are necessarily in this suite of bills, because they don't implicate foreign interference. These are offences that attach now to everyone, but in practice really to Commonwealth employees, and there's no nexus here between this legislation and any foreign agent or foreign person. To some extent, this is a standalone regime that in our view would benefit from a standalone piece of legislation, particularly given the complexity of the issues elsewhere in not only this bill but also the suite of legislation of which it is a part.[8]

4.13 At a public hearing, the Attorney-General's Department described the secrecy offences as 'an essential bedrock for the national security offences that sit above them'.[9] It explained that the Bill was responding to a 'large gap in the middle' between secrecy offences and espionage offences in the current law:

> What Commonwealth criminal law does have is espionage offences, but they represent the pinnacle of the criminal activity that occurs in this area, and then we have secrecy offences, which have been discussed this morning, which carry low penalties, haven't been updated in over 50 years and don't allow the [Australian Federal Police] to use their most important investigative tools. In the middle, which is where we understand most of the conduct falls, there are no criminal offences that would allow the passage of a matter being seen by an intelligence agency through to a criminal investigation.
>
> That's not the case in the counterpart countries that we've spoken to, where having a broad range of criminal offences that cover the full continuum of criminal conduct allows them to have investigative and prosecutorial

---

7 Dr Aruna Sathanapally, Director, Legal Policy, Human Rights Law Centre, *Committee Hansard*, Canberra, 30 January 2018, p. 55.

8 Dr Aruna Sathanapally, Director, Legal Policy, Human Rights Law Centre, *Committee Hansard*, Canberra, 30 January 2018, p. 57.

9 Ms Tara Inverarity, Assistant Secretary, Attorney-General's Department, *Committee Hansard*, Canberra, 31 January 2018, pp. 25–26.

> flexibility so that they can adopt the most appropriate criminal offence for wherever that is on the offending spectrum, which may be at the initial stages right through to the still very rare high-level espionage prosecutions. It allows them to take into account evidentiary issues where there may be challenges in proving a particular element. For example, the involvement of a foreign principal may be known to investigative agencies but difficult to prove with admissible evidence. What is essential from our perspective is having robust secrecy offences so that, if the link to a foreign principal can't be proved but the disclosure of highly sensitive material has occurred, there is still a strong prosecutorial option which carries a serious penalty which can punish that conduct but also act as a deterrent and show that you can't come to Australia and do these activities and not expect to have them matched by serious criminal penalties, if the right circumstances exist.[10]

Australian Law Reform Commission report

4.14 In outlining the need for reform, the Attorney-General's Department highlighted the Australian Law Reform Commission (ALRC)'s 2009 report, *Secrecy Laws and Open Government in Australia*.[11] This report is referred to several times in the Explanatory Memorandum,[12] and was also referred to by a large number of other submissions to the Committee's review.[13]

4.15 The ALRC's report was the product of a comprehensive review of secrecy laws and related issues that took place between August 2008 to December 2009. The Commission received submissions and consulted with a wide range of agencies, organisations and individuals.[14]

4.16 In its report, the ALRC recommended the repeal of the existing 'catch-all' secrecy offences in the Crimes Act and the introduction of a new 'general secrecy offence'. It's key recommendation for reform was that 'the sanctions

---

10 Ms Tara Inverarity, Assistant Secretary, Attorney-General's Department, *Committee Hansard*, Canberra, 31 January 2018, pp. 25-26.

11 Attorney-General's Department, *Submission 6*, p. 25.

12 Explanatory Memorandum, pp. 221-224, 231.

13 Lucy Strange, *Submission 4*, p. 1; Law Council of Australia, *Submission 5*, pp. 22, 56-58; Australian Lawyers for Human Rights, *Submission 7*, p. 4; Joint media organisations, *Submission 9*, p. 2; Human Rights Law Centre, *Submission 11*; Australian Human Rights Commission, *Submission 17*, p. 3; Dr Lawrence McNamara, *Submission 19*, p. 2; Joint councils for civil liberties, *Submission 31*, pp. 8–26.

14 Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, Report 112, December 2009, pp. 599-606.

of the criminal law … should be reserved for behaviour that harms, is reasonably likely to harm or intended to harm essential public interests'. In keeping with this principle, the ALRC recommended that the new general secrecy offence be limited to unauthorised disclosures that are likely to:

- damage the security, defence or international relations of the Commonwealth,
- prejudice the prevention, detection, investigation, prosecution or punishment of criminal offences,
- endanger the life or physical safety of any person, or
- prejudice the protection of public safety.[15]

4.17 The ALRC proposed that the new general secrecy offence apply to all Commonwealth information and all present and former Commonwealth officers. It recommended separate offences for the subsequent disclosure of Commonwealth information by third parties, where the information was initially disclosed in breach of the general secrecy offence or on terms requiring it to be held in confidence.[16]

4.18 The ALRC recommended that there should be exceptions (as opposed to defences) in the general secrecy offence for disclosure in the course of an officer's functions or duties; disclosure with the authority of an agency head or minister; and disclosure of information that is already lawfully in the public domain.[17]

4.19 The ALRC noted that, in addition to the general secrecy offence, there would still be a need for specific secrecy offences tailored to the needs of particular agencies or to the protection of certain kinds of information. The Commission made recommendations concerning the principles that should guide the creation of specific secrecy offences and the review of existing offences.[18]

---

15 Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, Report 112, December 2009, pp. 23-24.

16 Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, Report 112, December 2009, p. 24.

17 Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, Report 112, December 2009, p. 24.

18 Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, Report 112, December 2009, p. 24.

4.20 The Attorney-General's Department advised that the primary secrecy offences in the Bill were 'informed by' the ALRC report, in that they apply to communication (or other dealing) with information that is likely to cause harm. However, the Department acknowledged that the offences based on 'inherently harmful information', including security classified information, depart from the ALRC's recommendations.[19] The Department explained:

> The fundamental premise of the ALRC's consideration of secrecy laws was that disclosures that cause harm should be covered by the criminal law. From our perspective, we would argue that that is what we have implemented, although in a different form to what the ALRC envisaged in its report. We have taken the view that there are categories of information the release of which is inherently harmful, and that is reflected in the bill.[20]

4.21 A table comparing the secrecy provisions in the Bill to the model proposed by the ALRC is included at Appendix C. In summary, in addition to offences relating to 'inherently harmful information', the secrecy offences in the Bill depart from the ALRC's recommendations in the following ways:

- the general secrecy offences are applied to all persons, rather than only to Commonwealth officers (i.e. subsequent disclosures are not dealt with separately),
- a different definition of 'Commonwealth officer' is used,
- offence-specific defences, rather than exemptions, are provided in relation to conduct in the course of official functions or duties and information that is already public,
- the offences relating to 'inherently harmful information' and 'conduct causing harm to Australia's interests' (proposed section 122.2) apply to a broader range of information and interests than recommended by the ALRC,
- in addition to offences for communication, offences are created for dealing with information, removing information from a proper place of custody and failing to comply with direction regarding information,
- higher maximum penalties are imposed than was recommended by the ALRC, and
- existing section 70 of the Crimes Act is retained (in amended form), with no existing specific secrecy offences repealed.

---

19 Attorney-General's Department, *Submission 6*, pp. 30-31.

20 Ms Tara Inverarity, Assistant Secretary, Attorney-General's Department, *Committee Hansard*, Canberra, 31 January 2018, p. 28.

4.22 At a public hearing, the Department argued that it had followed the ALRC's report 'in spirit if not in letter':

> … although the offences in the bill do not exactly replicate the structure put forward by the ALRC, we have taken that as a guiding principle that harmful information is what should be targeted by the criminal law.[21]

4.23 Responding to a question about whether anything of material substance had changed since the ALRC report that would cause the Department not to follow the ALRC's recommendations, the Department noted:

> There have been a range of significant disclosures of information internationally since 2009, I believe, when the ALRC report was concluded that have brought into stark relief the consequences that can come from disclosure of information and the ease with which very large tranches of information can be disclosed.[22]

4.24 Other submitters to the inquiry were concerned by the Bill's departures from the ALRC's recommendations. The Human Rights Law Centre, for example, recommended that Schedule 2 be removed from the Bill and redrafted in line with the ALRC's recommendations.[23] The Centre's Dr Aruna Sathanapally told the Committee that while there would need to be coordination with the *Public Interest Disclosure Act 2013*, which was introduced since the ALRC's report, 'the bulk of the ALRC recommendations are still current and relevant and usable'.[24] Dr Sathanapally contended that, despite high-profile leaks of classified information in recent years,

> … the principles of maintaining a culture of transparency in government and maintaining a culture that government information is public information, unless there are reasons to the contrary, are things that endure and need to endure for the health of Australia's democracy. So, even though we of course need offences to deal with serious harm, we should make sure that our offences do deal with serious harm and don't end up compromising the real strides we've made since 1914 in terms of the health of Australia's democracy,

---

21 Ms Tara Inverarity, Assistant Secretary, Attorney-General's Department, *Committee Hansard*, Canberra, 31 January 2018, p. 28.

22 Ms Tara Inverarity, Assistant Secretary, Attorney-General's Department, *Committee Hansard*, Canberra, 31 January 2018, p. 28.

23 Human Rights Law Centre, *Submission 11*, p. ii.

24 Dr Aruna Sathanapally, Director, Legal Policy, Human Rights Law Centre, *Committee Hansard*, Canberra, 30 January 2018, p. 61.

> when section 70 was passed. While I appreciate that it has been eight years, I think that there are aspects of the ALRC's report that would have been timely in 1980.[25]

4.25 The Law Council of Australia similarly recommended that the proposed secrecy offences be 'amended in a manner which is consistent with the ALRC's secrecy report'.[26] Mr Morry Bailes, President of the Law Council, explained:

> We are concerned about three of the four offences being too broad and then turn to the fact that, given that the ALRC produced its report in relation to secrecy and made express findings, all of which, if adopted, would, in our respectful submission, address the difficulties with the Bill as it's currently drafted. We therefore recommend they be adopted and, again, in our respectful submission, that should not be construed as taking away from the effectiveness of the legislation. There is one instance where, if adopted, an offence would not be established, but it is a truer way of defining what the offences should be in our submission and would result in better law.[27]

4.26 The Human Rights Commissioner, Mr Edward Santow, noted that while the Bill replaces some older secrecy provisions in the Crimes Act, the Bill does not implement the ALRC's recommended 'overhaul of the approximately 500 secrecy provisions that exist across about 176 pieces of legislation'. Mr Santow urged that this overhaul be undertaken.[28]

Breadth of conduct captured by the offences

4.27 Many participants in the inquiry raised concerns about the breadth of conduct captured by the proposed secrecy offences. Specific concerns raised by participants are discussed below.

---

25 Dr Aruna Sathanapally, Director, Legal Policy, Human Rights Law Centre, *Committee Hansard*, Canberra, 30 January 2018, p. 61.

26 Law Council of Australia, *Submission 5*, p. 57.

27 Mr Morry Bailes, President, Law Council of Australia, *Committee Hansard*, Canberra, 30 January 2018, pp. 53–54.

28 Mr Edward Santow, Human Rights Commissioner, Australian Human Rights Commission, *Committee Hansard*, Canberra, 31 January 2018, p. 48.

Breadth of 'deal with' offences

4.28 Proposed section 122.1(2) makes it an offence to deal with, other than by communicating, 'inherently harmful information'. Similarly, proposed section 122.2(2) makes it an offence to deal with, other than by communicating, information in a way that does, will or is likely to cause harm to Australia's interests. For the purpose of these sections, 'deals with' is defined to apply when a person 'receives', 'obtains', 'collects', 'possesses', 'makes a record of', 'copies', 'alters', 'conceals', 'publishes' or 'makes information available'.[29]

4.29 Some participants in the inquiry raised concerns about the breadth of conduct captured by the term 'deals'. The joint media organisations, for example, submitted that the Bill would mean journalists, editorial and support staff are at risk of jail time as a result of merely having certain information in their possession:

> For example, a journalist receiving unsolicited information would be in automatic breach …
>
> Expanding on that, if the journalist received such information, how could the journalist determine whether the material is in breach without possessing, communicating, and otherwise dealing with it? A mere discussion of unsighted material might place journalists in breach, notwithstanding that they may then ask others about the information—with or without being in possession of a document.[30]

4.30 The joint media organisations highlighted the ALRC's view that 'the mere receipt or possession of information should not be covered in the general secrecy offence or the subsequent disclosure offences'.[31]

4.31 The Human Rights Law Centre considered that the breadth of the conduct captured by the offences is 'entirely inappropriate for general criminal offences across all types of information in an enormous range of contexts',[32]

---

29 Proposed section 90.1(1) of the *Criminal Code*.

30 Joint media organisations, *Submission 9*, p. 2.

31 Joint media organisations, *Submission 9*, p. 2; citing Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, Report 112, December 2009, p. 203.

32 Human Rights Law Centre, *Submission 11*, p. 17.

and similarly highlighted the Bill's discrepancy from the ALRC's recommendation.[33] The Centre further stated that it was

> not clear why 'dealing', as broadly defined, needs to be criminalised when preparatory offence provisions exist that would capture attempts to disclose or conspiracy to disclose information.[34]

4.32 The Attorney-General's Department explained at a hearing how each of the individual elements of the term 'deals' was arrived at:

> As you'll see in the offences, the communication is treated more seriously than the other dealings, but, in working closely with operational agencies about what they see in the threat environment, the list of matters that are covered by the definition of 'deals' reflects their advice on what is actually happening with information that falls within these offences. So, as part of the drafting process, each of those matters was carefully considered as to whether there were harmful case examples that fell within those categories.[35]

4.33 The Committee asked the Attorney-General's Department whether the inclusion of the words 'receiving', 'obtaining', 'collecting' and 'possessing' in the definition of 'deals' means that a person may have committed an offence simply by being given information that is, for example, security classified. In response, the Department noted that the fault element of 'intention' would apply to the physical element that a person communicated or otherwise dealt with information.[36] That is, section 5.2 of the *Criminal Code* provides that a person has 'intention' with respect to conduct if he or she 'means to' engage in that conduct.

4.34 As noted in the Explanatory Memorandum, to establish an offence under proposed section 122.1(2)—'other dealings with inherently harmful information'—the prosecution will need to prove beyond reasonable doubt that

- the person *intentionally* deals with information (other than by communicating it),
- either

---

33 Human Rights Law Centre, *Submission 11.2*, p. 5.

34 Dr Aruna Sathanapally, Director, Legal Advocacy, Human Rights Law Centre, *Committee Hansard*, Melbourne, 16 March 2018, p. 20.

35 Ms Tara Inverarity, Assistant Secretary, Attorney-General's Department, *Committee Hansard*, Melbourne, 16 March 2018, p. 39.

36 Attorney-General's Department, *Submission 6.1*, p. 58.

  - the information was inherently harmful information (other than security classified information) and the person was *reckless* as to this element, or
  - the information was security classified information, and
- the information was made or obtained by that or any other person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity and the person was *reckless* as to this element.[37]

4.35 The Law Council of Australia submitted that the secrecy offences required clarification 'to ensure that innocent receipt of information (e.g. in a filing cabinet) is not captured by the offence provisions':

> The link between the defendant's intention and the harmful behaviours targeted requires further precision. The limited news media exception may not be made out as it would be difficult for a defendant to demonstrate there was a reasonable belief in the public interest where they are in receipt of the information but have not had the opportunity to consider its contents.[38]

4.36 At a public hearing, the Law Council suggested that a possible solution would be to include a clause or note in the Bill that clarifies that innocent receipt of information is not covered by the secrecy offences.[39]

4.37 The Department explained that the offences would not apply in the situation of a person merely receiving and opening an envelope, or purchasing a filing cabinet, without any knowledge of what might be in it:

> [A] person who does not know what's in the envelope or does not know what's in the filing cabinet will not be able to commit this offence. They will not be reckless as to the specific nature of the information. So, the receipt is one element. All elements and all fault elements must be proved, and that factual scenario just will not satisfy the offence.[40]

4.38 In addition to its concerns about the innocent 'receipt' of information, the joint media organisations raised concerns about the use of other 'passive'

---

37 Explanatory Memorandum, p. 241.

38 Law Council of Australia, *Submission 5.1*, p. 2.

39 Dr David Neal SC, Member, National Criminal Law Committee, Law Council of Australia, *Committee Hansard*, Melbourne, 16 March 2018, p. 18.

40 Ms Tara Inverarity, Assistant Secretary, Attorney-General's Department, *Committee Hansard*, Melbourne, 16 March 2018, p. 43.

terms in definition of 'deal'. The organisations recommended that the terms 'receives', 'obtains', 'collects', 'possesses', 'makes a record of' and 'copies' be excluded from the operation of offences applying to non-Commonwealth officers.[41]

4.39 The Committee asked the Department whether 'deals with' would extend to a person intentionally viewing or downloading inherently harmful information that has been unlawfully published on the internet by another person. The Department provided the following response:

> The department thinks it unlikely that simply viewing information would fall within the definition of 'deals'. However, it would depend on the specific facts and circumstances of the case.
>
> The department notes that it is somewhat artificial to consider a situation of 'viewing' alone, as there would likely be other dealings with the information surrounding the viewing which may fall within the relevant definition.
>
> Depending on the facts and circumstances, downloading information may constitute 'possession' of information.[42]

Breadth of 'inherently harmful information' offences

4.40 'Inherently harmful information' is defined in proposed section 121.1 to include any of the following information:

a. security classified information,

b. information the communication of which would, or could reasonably be expected to, damage the security or defence of Australia,

c. information that was obtained by, or made by or on behalf of, a domestic intelligence agency or a foreign intelligence agency in connection with the agency's functions,

d. 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,

---

41 Joint media organisations, *Submission 9.2*, p. 4.

42 Attorney-General's Department, *Submission 6.1*, p. 58.

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

4.41 The Explanatory Memorandum states that this definition is intended to exhaustively list categories of information that

> are inherently harmful in the sense that
>
> - communicating such information,
> - otherwise dealing in such information ,
> - removing such information from, or holding such information outside, a proper place of custody for the information, or
> - failing to comply with a lawful direction regarding the retention, use or disposal of such information,
>
> will, or would reasonably be expected to, cause harm to essential public interests of the Commonwealth.[43]

4.42 Proposed section 122.1 creates underlying offences for each of these four types of activities.

4.43 A large number of submissions to the inquiry raised concerns about the scope and operation of the 'inherently harmful information' offences.[44] In many cases, submitters argued that conduct picked up by the term would not, in fact, be necessarily harmful. Submitters provided a range of examples of otherwise innocent conduct that may be inadvertently captured by these provisions.

4.44 Submitters also raised concerns about many of the specific components of the definition of 'inherently harmful information'.

---

43 Explanatory Memorandum, pp. 228–229.

44 Law Council of Australia, *Submission 5*, pp. 62-64; Australian Lawyers for Human Rights, *Submission 7*, pp. 4, 5; Joint media organisations, *Submission 9*, p. 3; Human Rights Law Centre, *Submission 11*, pp. 12-13; Australian Lawyers Alliance, *Submission 12*, p. 14; Australian Human Rights Commission, *Submission 17*, p. 4; Centre for Media Transition, University of Technology Sydney, *Submission 23*, p. 4; *Submission 26* (name withheld), pp. [1], [3]; United Nations Special Rapporteurs, *Submission 30*, pp. 5–7; Joint councils for civil liberties, *Submission 31*, pp. 10–18; Digital Rights Watch, *Submission 34*, p. [3].

Security classified information

4.45 Many submitters raised concerns about the inclusion of security classified information as paragraph (a) of the definition of 'inherently harmful information', including the appropriateness of applying serious criminal offences to security classified information, the lack of definition in the primary legislation, the application of strict liability, and the provision for evidentiary certificates issued by the Attorney-General. As these concerns are also relevant to the espionage offences in the Bill, these matters are discussed separately in Chapter 3.

Information relating to the security or defence of Australia

4.46 The Law Council of Australia noted that the term 'information the communication of which would, or *could reasonably be expected to*, damage the security or defence of Australia' provided for a lower standard than that recommended by the ALRC. The Law Council recommended that paragraph (b) be amended to read 'information the communication of which would, or *would be reasonably likely to*, damage the security or defence of Australia'.[45]

4.47 The Attorney-General's Department responded that it was 'not clear that the proposed change could make a material change to the definition'.[46]

4.48 The Human Rights Law Centre considered that, because it includes a harm-based test, it would be logical for paragraph (b) to be included in the definition of 'cause harm to Australia's interests' rather than the definition of 'inherently harmful information'.[47] The Attorney-General's Department agreed that moving this provision would make the provision somewhat more coherent, but noted that the definition within which it sits 'wouldn't make any practical difference'.[48]

---

45 Law Council of Australia, *Submission 5*, pp. 63-64.

46 Attorney-General's Department, *Submission 6.1*, pp. 20-21.

47 Human Rights Law Centre, *Submission 11*, pp. 4–5; Dr Aruna Sathanapally, Director of Legal Advocacy, Human Rights Law Centre, *Committee Hansard*, Melbourne, 16 March 2018, pp. 22–23.

48 Ms Tara Inverarity, Assistant Secretary, Attorney-General's Department, *Committee Hansard*, Melbourne, 16 March 2018, p. 59.

Information required to be provided to the Commonwealth by law

4.49 Several submitters considered the inclusion of paragraph (d)—'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'—to be inappropriate.[49] This category would include information required to be provided to a range of Commonwealth agencies and regulators, including:

- information that is required to be provided to the Australian Taxation Office by taxpayers in accordance with taxation legislation,
- information that is required to be provided to regulatory agencies, such as the Australian Securities and Investments Commission or the Australian Prudential Regulation Authority, under various regulatory regimes,
- information requirement to be provided by carriers and carriage service providers to the Communications Access Co-ordinator, in accordance with telecommunications interception legislation, and
- information obtained by Commonwealth authorities utilising coercive information gathering powers, including notices-to-produce, production orders, and compulsory questioning.[50]

4.50 The Attorney-General's Department explained:

> The purpose of paragraph (d) of the definition of 'inherently harmful information' is to ensure that information provided to the Commonwealth under a coercive power or other compulsion is protected. It is considered essential to protect such information where a person has been required to provide it to the Commonwealth, typically under compulsion or penalty for non-compliance. If this information is not adequately protected, it could have the impact of discouraging individuals and companies from providing honest and complete information to the Commonwealth in accordance with an obligation under a law or otherwise by compulsion of law. This harms the ability for Commonwealth authorities to perform their functions.[51]

4.51 The Human Rights Law Centre, however, contended:

---

49 Joint media organisations, *Submission 9*, p. 3; Human Rights Law Centre, *Submission 11*, p. 12; Centre for Media Transition, University of Technology Sydney, *Submission 23*, p. 4; Joint councils for civil liberties, *Submission 31*, p. 14.

50 Explanatory Memorandum, p. 230.

51 Attorney-General's Department, *Submission 6.1*, pp. 59-60.

> It is acknowledged that the unauthorised disclosure of information provided to Commonwealth authorities, in certain circumstances, could prejudice the effective operation of government, or personal privacy. However, … other tools are readily available to deal with that policy problem. The criminal law is neither necessary nor proportionate.[52]

4.52 Similarly, the Centre for Media Transition at the University of Technology, Sydney, argued that the 'vast amount' of information that could fall under this part of the term 'inherently harmful' would make the term 'almost meaningless'. The Centre explained:

> The Explanatory Memorandum gives the example of the requirement on carriers and carriage service providers to give information to the Communications Access Co-ordinator in accordance with telecommunications interception legislation. This is a security-related example and may well be justified. But telecommunications companies are also required to provide substantial amounts of information to the [Australian Communications and Media Authority (ACMA)] and the [Australian Competition and Consumer Commission] under legislation which has no connection with security—for example, the consumer protection matters arising under the *Telecommunications (Consumer Protection and Service Standards) Act 1999*. In the case of the media ownership and control rules mentioned above, under sections 63 and 64 of the [*Broadcasting Services Act 1992* (BSA)] a person who comes into a position to exercise control of a broadcasting licence must submit a notification to that effect to the ACMA, as must the licensee of that service. Similarly, broadcasters are required under the BSA to provide information concerning program content to the ACMA. None of this has a connection with espionage.[53]

Information relating to law enforcement agencies

4.53 One submission to the inquiry expressed concern that paragraph (e) of the definition of 'inherently harmful information'—information relating to the operations, capabilities or technologies of, or methods or sources used by, a domestic or foreign law enforcement agency—was 'so broad as to be draconian'. The submitter considered that the paragraph could 'curtail any scrutiny or public accountability of law enforcement agencies or their activities', and 'could also create great difficulty to a defendant in a criminal

---

52 Human Rights Law Centre, *Submission 11*, p. 12.

53 Centre for Media Transition, University of Technology Sydney, *Submission 23*, p. 4.

matter, where their defence relies [on] any sort of law enforcement operational information'. The submitter explained:

> Even routine traffic policing could be construed as an 'operation' of a domestic law enforcement agency. If for example I were to be stopped for a random breath test, and if I were to tell anyone of my interaction with the police, in doing so I would likely commit the offence of 'communicating inherently harmful information'; the 'harmful information' in this case being information about a domestic law enforcement 'operation'.[54]

4.54 The joint councils for civil liberties similarly noted that while

> [t]his category is appropriate in that it would capture much sensitive, inherently harmful information whose unlawful communication would cause harm to law enforcement agencies operations and capacities and Australia's essential interests

it would also capture

> much information that will have no significant bearing upon the effective operation of law enforcement agencies and is not likely to harm Australia's essential interests.[55]

4.55 The Explanatory Memorandum notes that a person would not be subject to criminal liability for communicating or otherwise dealing with such information in circumstances covered by the defences in section 122.5. In particular, the Explanatory Memorandum notes that proposed subsection 122.5(2) provides a defence where information has already been communicated or made public with the authority of the Commonwealth. The Explanatory Memorandum states:

> The concept of making information available to the public includes making information to a relevant segment of the public, and can include making information available to a single person, for example where an operation is conducted in public but witnessed only by a single person. As a result, the inclusion of law enforcement operations within the definition of inherently harmful information is not intended to have the effect of extending criminal liability to persons who communicate information about public law enforcement operations.[56]

---

54 *Submission 26* (name withheld), p. [3].

55 Joint councils for civil liberties, *Submission 31*, pp. 14–15.

56 Explanatory Memorandum, p. 231.

Information related to foreign law enforcement and intelligence agencies

4.56 The Human Rights Law Centre submitted that it was 'far from clear' that disclosure of the information of a foreign law enforcement agency or a foreign intelligence agency, as provided for in paragraphs (c) and (e) of the definition of 'inherently harmful information', would inherently damage Australia's interests.[57] The joint councils for civil liberties similarly recommended that the reference to foreign intelligence agencies be removed from paragraph (c).[58]

4.57 The Law Council of Australia recommended that provisions relating to foreign agencies be redrafted to make it clear that the information would, or would be reasonably likely to, harm one of the four essential public interests identified by the ALRC in its Secrecy Report.[59]

4.58 The Explanatory Memorandum provides the following explanation of why disclosure of intelligence-related information is considered to be particularly sensitive:

> The compromise of information made or obtained by the intelligence services could reasonably be expected to cause serious damage to Australia's national security. Even small amounts of such information could, when taken together with other information, compromise national security, regardless of the apparent sensitivity of the particular information—this is referred to as the 'mosaic approach' to intelligence collection.
>
> For example, even seemingly innocuous pieces of information, such as the amount of leave available to staff members or their salary, can yield significant counterintelligence dividends to a foreign intelligence service.[60]

4.59 The particularly sensitive nature of information obtained or generated by intelligence agencies was recognised by the ALRC in its 2009 report. Although not supporting their inclusion in a general secrecy offence, the ALRC expressed the view that specific secrecy offences prohibiting the disclosure of information obtained or generated by intelligence agencies—without the need to prove harm in every case—are justified by the sensitive

---

57 Human Rights Law Centre, *Submission 11*, p. 13.

58 Joint councils for civil liberties, *Submission 31*, p. 14.

59 Law Council of Australia, *Submission 5*, pp. 63-64.

60 Explanatory Memorandum, p. 229.

nature of the information and the special duties and responsibilities of officers and others who work in and with such agencies.[61]

4.60 In relation to information provided by foreign agencies, the Attorney-General's Department argued such information is considered inherently harmful 'because of the adverse effect it can have on law enforcement and intelligence cooperation':

> If foreign agencies share information with Australia, particularly about their most sensitive operations and techniques, it is essential that it can be appropriately protected. If this information sharing were withdrawn, there would be significant adverse consequences for Australia's national interest.[62]

Government proposed amendments – inherently harmful information

4.61 On 13 February 2018, the Attorney-General's Department advised the Committee that it had been asked by the Attorney-General to progress a number of changes to the general secrecy offences in Schedule 2 to the Bill. This included amendments to 'improve the clarity of offences that apply to current and former Commonwealth officers, most particularly by narrowing the definitions of "causes harm to Australia's interests" and "inherently harmful information" at section 121.1 of the Bill'. The Committee received draft amendments to this effect from the Attorney-General on 5 March 2018.[63] The proposed amendments in relation to 'inherently harmful information' included:

- limiting 'security classified information' in paragraph (a) to classifications of SECRET or TOP SECRET, or equivalent classifications or markings prescribed by regulations (as noted in Chapter 3),
- removing strict liability in relation to security classifications, and
- entirely removing paragraph (d)—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'—from the definition.

---

61 Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, Report 112, December 2009, pp. 288–289.

62 Attorney-General's Department, *Submission 6.1*, p. 20..

63 Attorney-General, *Submissions 40 and 41*.

4.62 The proposed amendments were generally supported by participants in the inquiry.[64]

4.63 The Law Council of Australia did not oppose the removal of paragraph (d) from the definition, but submitted that it 'would be grateful for further clarification from the Attorney-General's Department as to its purpose'.[65]

Breadth of 'cause harm to Australia's interests' offences

4.64 The phrase 'cause harm to Australia's interests' is defined in proposed section 121.1 to mean to:

> (a) interfere with or prejudice the prevention, detection, investigation, prosecution or punishment of:
>
> > (i) a criminal offence against; or
> >
> > (ii) a contravention of a provision, that is subject to a civil penalty, of:
> >
> > a law of the Commonwealth; or
>
> (b) interfere with or prejudice the performance of functions of the Australian Federal Police (AFP) under:
>
> > (i) paragraph 8(1)(be) of the *Australian Federal Police Act 1979* (protective and custodial functions); or
> >
> > (ii) the *Proceeds of Crime Act 2002*; or
>
> (c) harm or prejudice Australia's international relations in relation to information that was communicated in confidence:
>
> > (i) by, or on behalf of, the government of a foreign country, an authority of the government of a foreign country or an international organisation; and
> >
> > (ii) to the Government of the Commonwealth, to an authority of the Commonwealth, or to a person receiving the communication on behalf of the Commonwealth or an authority of the Commonwealth; or
>
> (d) harm or prejudice Australia's international relations in any other way; or

---

64 Law Council of Australia, *Submission 5.1*, p. 3; Human Rights Law Centre, *Submission 11*, p. 3; Joint councils for civil liberties, *Submission 31*, p. 6.

65 Law Council of Australia, *Submission 5.1*, p. 4.

(e) harm or prejudice relations between the Commonwealth and a State or Territory; or

(f) harm or prejudice the health or safety of the public or a section of the public.

4.65 As listed above, proposed section 122.2 creates four underlying offences for communicating, dealing with, removing from a proper place of custody or failing to comply with a lawful direction in relation to information in a way that 'causes harm to Australia's interests'.

4.66 Various submitters to the inquiry raised concerns about the breadth of conduct captured by the offences in proposed section 122.2, and queried whether certain elements of the definition were appropriate.[66]

Interference with or prejudicing criminal investigations

4.67 The Centre for Media Transition at the University of Technology, Sydney, submitted that paragraph (a) of the definition of 'cause harm to Australia's interests' would capture 'matters that are properly the subject of secrecy laws, but would also cover matters that are not'. The Centre cited an example of a journalist investigating media ownership arrangements, including the actions of the Australian Communications and Media Authority.[67]

Interference versus damage or prejudice

4.68 The Law Council of Australia noted that paragraphs (a) and (b) of the definition required mere 'interference' rather than damage or prejudice. The Law Council considered this to be a 'much lower' threshold, which 'may extend to a broad range of conduct, including innocuous conduct'. The Law Council recommended that the phrase 'interfere with' be removed from the

---

66 Law Council of Australia, *Submission 5*, pp. 59–62; Australian Lawyers for Human Rights, *Submission 7*, pp. 4–5; Joint media organisations, *Submission 9*, p. 3; Human Rights Law Centre, *Submission 11*, p. 14; Australian Lawyers Alliance, *Submission 12*, pp. 13–14; Australian Human Rights Commission, *Submission 17*, p. 4; Centre for Media Transition, University of Technology, Sydney, *Submission 23*, pp. 2–4; United Nations Special Rapporteurs, *Submission 30*, p. 7; Joint councils for civil liberties, *Submission 31*, pp. 20–23, Nyman Gibson Miralis, *Submission 35*, p. 5; Digital Rights Watch, *Submission 34*, p. [3]; GetUp, *Submission 38*, p. 3; Dr Luke Beck, Associate Professor, Faculty of Law, Monash University, *Submission 41*, p. 2.

67 Centre for Media Transition, University of Technology, Sydney, *Submission 23*, p. 3.

paragraphs.[68] A similar point was made by the joint councils for civil liberties.[69]

4.69 The Attorney-General's Department disagreed with the Law Council's recommendation, arguing that it was important for the secrecy offences to cover 'interference' not only 'prejudice' to those functions:

> If the offences did not cover 'interference', the AFP would have to wait for a criminal investigation to actually be prejudiced before being able to investigate the matter as a secrecy offence. This creates risks to the Commonwealth that can be avoided if the AFP is able to intervene at an earlier stage, when the person's conduct is 'interfering with' (but has not yet actually prejudiced) a criminal investigation.[70]

4.70 At a public hearing, the Law Council elaborated that its concern with the term 'interference with' was the potential for it to 'impact on freedom of speech in relation to, for example, prosecution malpractice issues'.[71]

Civil penalty contraventions and proceeds of crime legislation

4.71 Several submitters expressed concern about subparagraph (a)(ii) and (b)(ii) of the definition of 'causes harm', which extends to information relating to civil penalty proceedings and the AFP's functions under the *Proceeds of Crime Act 2002*.[72] Submitters highlighted the ALRC's view that

- the general criminal offence should not cover unauthorised disclosures of information that would prejudice the prevention, detection, investigation, prosecution or punishment of a breach of a law imposing penalties or sanctions that are not criminal, and
- the general criminal offence should not extend to unauthorised disclosures of information that would prejudice the enforcement of laws

---

68 Law Council of Australia, *Submission 5*, pp. 59–60, 62.

69 Joint councils for civil liberties, *Submission 31*, p. 22.

70 Attorney-General's Department, *Submission 6.1*, p. 18.

71 Dr Natasha Molt, Deputy Director of Policy, Policy Division, Law Council of Australia, *Committee Hansard*, Melbourne, 16 March 2018, p. 17.

72 Law Council of Australia, *Submission 5*, pp. 60–61; Joint media organisations, *Submission 9*, p. 3; Human Rights Law Centre, *Submission 11*, p. 14; Joint councils for civil liberties, *Submission 31*, p. 20; Nyman Gibson Miralis, *Submission 35*, p. 5.

> relating to the confiscation of the proceeds of crime, or the protection of the public revenue.[73]

4.72 The ALRC recommended that, in certain circumstances in which the disclosure of such information may warrant criminal sanctions, specific offences could be used to protect the investigatory process.[74]

4.73 The Law Council of Australia recommended that the phrase 'contravention of a provision, that is subject to a civil penalty, of' be removed from proposed subparagraph 121.1(1)(a)(ii), or that, as a minimum, the provision be limited to contraventions of serious Commonwealth civil penalty provisions which attract an equivalent civil penalty of 3 years imprisonment.[75]

4.74 Responding to this recommendation, the Attorney-General's Department referred to the Explanatory Memorandum's account of why the Bill departs from the ALRC's model to include civil penalty provisions:

> When read together with the offence provision in section 122.2, the use of official information to interfere with or prejudice the effective enforcement of a civil penalty provision involves a serious interference with the administration of justice, as well as an improper use of official information that is likely to undermine public confidence in the effective administration of justice. Accordingly, such conduct should be subject to criminal liability.[76]

4.75 The Law Council also recommended that the *Proceeds of Crime Act 2002* be removed from proposed subparagraph 121.1(1)(b)(ii).[77] It noted that

> the ALRC, in its report, fairly clearly spelt out that that should be covered, if it's needed at all, by a specific secrecy offence rather than in the general secrecy offences which we have here.[78]

---

73 Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, Report 112, December 2009, pp. 157–158.

74 Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, Report 112, December 2009, p. 159.

75 Law Council of Australia, *Submission 5*, p. 62.

76 Explanatory Memorandum, p. 222. See also Attorney-General's Department, *Submission 6.1*, p. 18.

77 Law Council of Australia, *Submission 5*, p. 62.

78 Dr Natasha Molt, Deputy Director of Policy, Policy Division, Law Council of Australia, *Committee Hansard*, Melbourne, 16 March 2018, p. 17.

4.76 In relation to the proceeds of crime legislation, the Explanatory Memorandums states:

> [T]he POCA [*Proceeds of Crime Act 2002*] establishes a civil forfeiture scheme to confiscate unlawfully acquired property, as well as associated powers such as asset freezing. Strong and effective action to confiscate proceeds of crime assists in attacking the profit-motive of organised crime, including illicit activities involving drug trafficking, people smuggling, money laundering and large-scale fraud. The effective performance of the Australian Federal Police's functions under the POCA is an essential public interest.
>
> … The ALRC considered that it would be more appropriate to rely on specific secrecy provisions in sections 210, 217 and 223 [of] the POCA (which relate to the unauthorised disclosure of information about production orders, notices to financial institutions and monitoring orders). However, those specific secrecy provisions cover only a subset of the kinds of official information that could be improperly communicated to interfere with or prejudice the performance of the Australian Federal Police's functions under the POCA, and the associated, essential public interests.[79]

4.77 Responding to the Law Council's recommendation, the Attorney-General's Department added:

> It is appropriate for the AFP's functions under the POCA to be covered in this definition. Strong action to confiscate proceeds of crime assists in attacking the profit motive of organised crime, and the effective performance of these functions is an essential public interest.[80]

Australia's international relations and relations with states and territories

4.78 The inclusion of harm or prejudice to Australia's international relations [paragraphs (c) and (d)] and relations between the Commonwealth and a State or Territory [paragraph (e)] also attracted comment from submitters.[81]

4.79 The Centre for Media Transition, for example, submitted that the inclusion of 'an international organisation' in paragraph (c) would extend the laws to

---

79 Explanatory Memorandum, p. 223.

80 Attorney-General's Department, *Submission 6.1*, p. 19.

81 Law Council of Australia, *Submission 5*, pp. 61–62; Joint media organisations, *Submission 9*, pp. 3–4; Human Rights Law Centre, *Submission 11*, p. 14; Centre for Media Transition, University of Technology, Sydney, *Submission 23*, pp. 3–4; Joint councils for civil liberties, *Submission 31*, pp. 20–22.

'any number of entities which might provide information that is confidential but does not concern matters of national security'.[82]

4.80 The joint media organisations suggested that reporting on international trade or relations between the Commonwealth and states in relation to Goods and Services Tax distributions could be captured.[83]

4.81 The Human Rights Law Centre was concerned that the inclusion of paragraphs (d) and (e) of the definition means that proposed section 122.2

> criminalises, with very severe penalties, information that could clearly be a matter of considerable, legitimate public interest, and it is easy to imagine that it would include information that the principles of open government—and the constitutional protection for political communication—would require be freely shared and communicated.[84]

4.82 The Explanatory Memorandum to the Bill notes that the term 'international relations' has the meaning given in section 10 of the *National Security Information (Criminal and Civil Proceedings) Act 2004*, which is 'political, military and economic relations with foreign governments and international organisations'. It states that the concept of harming or prejudicing Australia's international relations includes things such as:

- the lessening or cessation of military or intelligence cooperation,
- damage to Australia's negotiating position in respect of a treaty or agreement, or within an international organisation such as the United Nations or an organ thereof,
- a reduction in the quality or [quantity] of information provided by a foreign government or international organisation,
- loss of confidence or trust in the Australian Government by an overseas government or international organisation,
- a detrimental impact on the ability of the Australian Government to maintain good working relations with a foreign government or international organisation, or

82 Centre for Media Transition, University of Technology, Sydney, *Submission 23*, p. 3.

83 Joint media organisations, *Submission 9*, pp. 3–4.

84 Human Rights Law Centre, *Submission 11*, p. 14.

- intangible damage to Australia's reputation or relationships between the Australian Government and a foreign government or international organisation, or between officials,

having the effect of diminishing the capacity of the Australian Government to function in the global political, military and economic environment.[85]

4.83 The Explanatory Memorandum states that the concept of harming or prejudicing relations between the Commonwealth and a State or Territory includes things such as:

- the lessening or cessation of law enforcement cooperation,
- a reduction in the quality or [quantity] of information provided by a State or Territory,
- loss of confidence or trust in the Commonwealth Government by a State or Territory Government,
- a detrimental impact on the ability of the Commonwealth Government to maintain good working relations with a State or Territory Government, or
- intangible damage to Australia's reputation or relationships between the Commonwealth Government and a State or Territory Government, or between officials

having the effect of diminishing the capacity of the Commonwealth Government, or State or Territory Government, to function within Australia's federal structure.[86]

4.84 The Law Council of Australia recommended that, for the purposes of paragraphs (d) and (e), the Explanatory Memorandum should clarify what may amount to 'intangible damage'.[87] In response, the Attorney-General's Department submitted:

> The reference to 'intangible' damage to Australia's reputation or relationships is intended to cover situations where Australia's international standing is reduced in ways that are real, but not able to be specifically and individually listed. This is consistent with the ordinary meaning of the word.[88]

---

85 Explanatory Memorandum, pp. 224-225.

86 Explanatory Memorandum, pp. 225-226.

87 Law Council of Australia, *Submission 5*, p. 62.

88 Attorney-General's Department, *Submission 6.1*, p. 19.

Government proposed amendments – cause harm to Australia's interests

4.85 On 13 February 2018, the Attorney-General's Department advised the Committee that it had been asked by the Attorney-General to progress a number of changes to the general secrecy offences in Schedule 2 to the Bill. This included amendments to 'improve the clarity of offences that apply to current and former Commonwealth officers, most particularly by narrowing the definitions of "causes harm to Australia's interests" and "inherently harmful information" at section 121.1 of the Bill'. The Committee received draft amendments to this effect from the Attorney-General on 5 March 2018.[89] The proposed amendments in relation to the definition of 'causes harm to Australia's interests' included:

- removing provisions subject to civil penalties from paragraph (a) of the definition,
- entirely removing paragraph (d)—'harm or prejudice Australia's international relations in any other way',
- entirely removing paragraph (e)—'harm or prejudice relations between the Commonwealth and a State or Territory, and
- limiting paragraph (f) to harm or prejudice to the health or safety of the *Australian* public, or a sections of the *Australian* public.

4.86 The proposed amendments were generally supported by participants in the inquiry.[90] The Human Rights Law Centre submitted, for example, that the amendments would 'narrow the list of interests in the definition … to only those interests that are appropriately captured within a general secrecy offence'.[91]

4.87 The Law Council of Australia, while welcoming the amendments, noted that the phrase 'interfere with' would remain in the amended paragraph (a). It therefore considered the paragraph 'remains very broad and may well stifle criticism of police, security or prosecution officials who have acted improperly or negligently'. The Law Council also reiterated its concern about proceeds of crime matters falling within the proposed definition.[92]

---

89 Attorney-General, *Submission 40*.

90 Law Council of Australia, *Submission 5.1*, p. 3; Human Rights Law Centre, *Submission 11*, p. 1; Joint councils for civil liberties, *Submission 31*, p. 7.

91 Human Rights Law Centre, *Submission 11*, p. 1

92 Law Council of Australia, *Submission 5.1*, p. 3.

4.88 The joint councils for civil liberties similarly noted that while the deletions 'lessen the overreach of the offence and are a significant improvement', further amendments were required to align the offence more fully with the ALRC's recommendation.[93]

'Proper place of custody' offences

4.89 Proposed subsections 122.1(3) (relating to inherently harmful information) and 122.2(3) (relating to conduct causing harm to Australia's interests) make it an offence to remove information from, or hold information outside, a 'proper place of custody for the information.

4.90 Proposed section 121.2 provides that the meaning of the term 'proper place of custody' will be prescribed in regulations. The Explanatory Memorandum states that the term should be 'interpreted broadly' and for specified information may include, for example,

- a building or part of a building,
- a safe, compactus or other place of storage,
- a briefcase, bag or other container allowing for the custody of information or documents in transit, or
- an electronic system, computer network, computer or device allowing for the custody of information in electronic form.[94]

4.91 The Explanatory Memorandum further states that the regulations may prescribe that a proper place of custody must meet certain requirements.[95]

4.92 The Law Council of Australia recommended that the type of information that may be 'proper place of custody' be more clearly defined an circumscribed in the Bill. It suggested that 'appropriate criteria' be incorporated to 'assist in ensuring that the matter would, or would be reasonably likely to cause harm to or prejudice Australia's national security'.[96]

4.93 The Commonwealth Ombudsman, Michael Manthorpe PSM, noted that his office would hold 'inherently harmful information'. He submitted:

---

93 Joint councils for civil liberties, *Submission 31*, p. 7.

94 Explanatory Memorandum, p. 233.

95 Explanatory Memorandum, p. 233.

96 Law Council of Australia, *Submission 5*, p. 65.

> Without a definition of 'proper place of custody' it 'is not clear what resourcing or other practical implications this requirement may have on my office.[97]

4.94 The Attorney-General's Department provided the following response to this concern:

> The department notes that most, if not all, Commonwealth departments and agencies will hold inherently harmful information. This information is already required to be stored and dealt with in accordance with the Commonwealth's protective security policies.
>
> The definition of 'proper place of custody' will reflect the requirements of these protective security policies. There will be no additional burden on departments and agencies that are already complying with protective security policies.
>
> The secrecy offences in the Bill are subject to delayed commencement and will commence by Proclamation, within six months of the Bill receiving the Royal Assent. The department intends to consult departments and agencies about the definition of proper place of custody during this period.[98]

4.95 The Department advised that draft regulations had not yet been prepared, but would be prepared consistently with the approach set out in the Explanatory Memorandum.[99]

'Lawful direction' offences

4.96 Proposed subsections 122.1(4) (relating to inherently harmful information) and 122.2(4) (relating to conduct causing harm to Australia's interests) make it an offence for a person to fail to comply with a lawful direction regarding the retention, use or disposal of information.

4.97 The Explanatory Memorandum describes intent of these offences:

> It is intended that the concept of a lawful direction include a direction that is lawful, from a person with the authority to give that direction. It is not intended that there must exist a formal relationship of command or control

---

97 Commonwealth Ombudsman, *Submission 8*, pp. 4-5.

98 Attorney-General's Department, *Submission 6.1*, p. 27.

99 Attorney-General's Department, *Submission 6.1*, p. 56.

between the person who gives the direction and the person to whom the direction is given. Examples of a lawful direction would include:

- Example 1: Person A is an [Australian Public Service (APS)] employee. Person B is an APS employee of the same agency. Person B gives Person A a direction, and has the authority to give that direction.
- Example 2: Person C is subject to an arrangement or agreement with the Commonwealth, or a Commonwealth entity. Person D gives Person C a direction, and has the authority to give that direction in connection with the arrangement or agreement.
- Example 3: Person E gives Person F information. In the course of giving the information to Person F, Person E gives Person F a direction.[100]

4.98 The Explanatory Memorandum also provides the following example of where the offence would be committed:

> Person A is employed under the Members of Parliament (Staff) Act 1984. Person A is given a document containing an update on an ongoing criminal intelligence investigation by Person B, a senior official of the Australian Criminal Intelligence Commission [ACIC]. The document contains information obtained using the ACIC's coercive examination powers, and from a source. Person B directs Person A to store the document in a safe that only Person A has access to. Person A stores the document in a safe that is accessible by all staff in the office.[101]

4.99 The Inspector-General of Intelligence and Security (IGIS) noted that the term 'lawful direction' is not defined in the Bill, 'nor is there any specific limitation on who may make these directions or the content of directions beyond the broad subject matter to which they must relate'. The IGIS pointed out a risk of unintended consequences from applying criminal liability to the contravention of such directions. The IGIS stated that

> a broad class of people (including presumably most or all supervisors) will have the ability to give directions which will effectively criminalise behaviour. Such directions may well be lawful but, in my view, it does not necessarily follow from the mere fact that a direction is lawful that there is an appropriate basis for applying criminal liability to contraventions of all such directions. The proposed offence could attach significant criminal sanctions to the breach of directions that are of a relatively trivial nature and do not, in fact, raise any

100 Explanatory Memorandum, pp. 249-250.

101 Explanatory Memorandum, p. 248.

> realistic prospect of the relevant information being placed at risk of compromise.
>
> There is also a risk that the application of criminal sanctions to any and all such directions may engender a punitive and defensive approach towards security compliance. This may create reluctance on the part of some officers to proactively disclose and report breaches, and may lead to the concealment of compliance issues out of fear of exposure to criminal penalty.[102]

4.100 The IGIS suggested that consideration could be given to whether further statutory parameters could be applied to the concept of 'lawful direction' in order to 'help to ensure that the proposed criminal law response is proportionate to the wrongdoing sought to be targeted, is not unduly reliant on administrative discretion to achieve this objective'.[103]

4.101 The Attorney-General's Department provided the following response:

> The department does not agree with the assertion that breach of such directions are necessarily 'relatively trivial', when taking into account the nature of the information covered by the offences.
>
> The onus will be on the prosecution to prove, beyond a reasonable doubt, that there was a lawful direction. The prosecution will also have to prove that the defendant was reckless as to this element.[104]

4.102 In a supplementary submission, the IGIS reiterated her support for further statutory parameters to be applied to the concept of a 'lawful direction', in particular a requirement that the direction was issued 'for the purpose of protecting the security of the information against unauthorised access or disclosure'.[105]

4.103 The IGIS considered that it was conceivable that a direction about the use, retention or disposal of information 'may have no bearing upon the protection of the security of that information'. She provided the following examples:

---

102 Inspector-General of Intelligence and Security, *Submission 13*, p. 9.

103 Inspector-General of Intelligence and Security, *Submission 13*, p. 9.

104 Attorney-General's Department, *Submission 6.1*, p. 38.

105 Inspector-General of Intelligence and Security, *Submission 13.2*, p. 10.

- A direction to store a document of a particular classification (such as SECRET) in one safe and not another, purely for reasons of convenience of access by authorised persons within an agency. Each safe could possess the same security specifications (for example, 'Class B') and could be subject to identical access controls that restrict access to the same persons, all of whom are authorised to access the relevant information.
- A direction to contact another person at, or by, a particular time and disseminate a piece of security classified information that is relevant to the sending and receiving agencies' functions, although the appointed deadline is not critical to the performance of those functions. (Noting that the 'use' of information could conceivably cover its dissemination.)[106]

Aggravated offences

4.104 The underlying secrecy offences in proposed sections 122.1 and 122.2 carry penalties of up to 15 years imprisonment (for communication offences) or five years imprisonment (for dealing with, proper place of custody, or lawful direction offences). Proposed section 122.3 provides that aggravated offences, carrying an additional five years imprisonment, have been committed if any of the following circumstances exist in relation to an underlying offence:

> (i) the information in relation to which the underlying offence is committed (the relevant information) has a security classification of secret or above;
>
> (ii) if the commission of the underlying offence involves a record containing the relevant information—the record is marked with a code word, "for Australian eyes only" or as prescribed by the regulations for the purposes of this subparagraph;
>
> (iii) the commission of the underlying offence involves 5 or more records each of which has a security classification;
>
> (iv) the commission of the underlying offence involves the person altering a record to remove or conceal its security classification;
>
> (v) at the time the person committed the underlying offence, the person held an Australian Government security clearance.

106 Inspector-General of Intelligence and Security, *Submission 13.2*, p. 10.

4.105 The appropriateness of attaching criminal liability to security classifications [subparagraphs (i), (iii) and (iv)], and related matters concerning security classifications, are discussed in Chapter 3.

4.106 The definition of 'Australian Government security clearance' [subparagraph (v)] is discussed in Chapter 3. The Human Rights Law Centre submitted that it was 'troubling' that the fact that a person held any security clearance, even at the lowest levels, is proposed to be an aggravating circumstance, 'with no need for their security clearance to be connected in any way to the offence'.[107] The joint councils for civil liberties similarly noted that some clearances give access to only a very limited set of information, and argued that this as 'not a sufficiently discriminating criterion to justify the aggravated penalty'.[108]

4.107 In relation to subparagraph (ii), the Committee asked the Department to clarify what the regulations relating to code words are intended to cover, including whether the provision would allow any code word to be prescribed by the regulations, or only those which have the same meaning and effect as the label 'for Australian eyes only'. The Department clarified that a code word 'will not need to be prescribed in the regulations' in order for the aggravating circumstance to apply:

> The aggravating circumstance in subparagraph 122.3(1)(b)(ii) will apply if the underlying offence involves a record and the record:
>
> - is marked with a code word
> - is marked with 'for Australian eyes only'
> - is marked as prescribed by the regulations for the purposes of this subparagraph.[109]

4.108 The joint councils for civil liberties recommended that the aggravated offences in proposed section 122.3 be removed from the Bill entirely, noting that 'the aggravating factors and the likely harm that would result from the aggravating conduct are not substantially different from that covered in the underlying offences'.[110]

---

107 Human Rights Law Centre, *Submission 11*, p. 20.

108 Joint councils for civil liberties, *Submission 31*, p. 25.

109 Attorney-General's Department, *Submission 6.1*, pp. 56-57.

110 Joint councils for civil liberties, *Submission 31*, p. 25.

Government proposed amendments – aggravated offences

4.109 In amendments received by the Committee on 5 March 2018, the Attorney-General proposed removing aggravating factor (i)—'a security classification of secret or above'—as a consequence of the proposed amendments which limit the definition of 'security classified information' to information classified SECRET or TOP SECRET, or equivalent (as noted above and in Chapter 3).[111]

Application to 'insiders' and 'outsiders'

4.110 A number of participants in the inquiry were concerned that the secrecy offences in the Bill would apply equally to Commonwealth officers and all other persons.[112]

4.111 As summarised above, the ALRC has recommended that there be a general secrecy offence for unauthorised disclosure of information by Commonwealth officers, with separate 'subsequent disclosure' offences for non-Commonwealth officers.

4.112 This distinction was supported by Independent National Security Legislation Monitor, the Hon. Roger Gyles AO QC, in his 2015 review of the secrecy offence in section 35P of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) regarding special intelligence operations (SIOs). Mr Gyles recommended that the existing section 35P be redrafted to treat 'insiders' (in that case, ASIO officers and affiliates) and 'outsiders' (third parties, such as journalists) separately, with one part dealing with third parties and another part dealing with insiders. The offences for 'outsiders' would carry the same penalties as for 'insiders', but with additional physical elements required to be proven.[113] Mr Gyles' recommendations were accepted by the Government and enacted following the passage of the Counter-Terrorism Legislation Amendment Bill 2016. Mr Gyles explained the reasons for treating insiders and outsiders separately as follows:

---

111 Attorney-General, *Submission 40.1*, p. 4 (amendment No. 32).

112 Law Council of Australia, *Submission 5*, pp. 55, 57; Joint media organisations, *Submission 9*, p. 2; Human Rights Law Centre, *Submission 11*, p. 16; Human Rights Law Centre, *Submission 17*, pp. 3–4; Joint councils for civil liberties, *Submission 31*, pp. 9, 28.

113 Independent National Security Legislation Monitor, *Report on the impact on journalists of section 35P of the ASIO Act*, October 2015, p. 3.

> The principal differences between insiders and outsiders lie in the means of knowledge about an SIO and the obligations of confidentiality owed by insiders. An outsider has no direct means of knowledge and owes no duty of confidence. Unless good cause is shown, it is not acceptable that an outsider, without any duty of confidentiality, should have to risk criminal conviction for publication made without any or any reliable knowledge of the existence or nature of an SIO.[114]

4.113 Dr Aruna Sathanapally of the Human Rights Law Centre similarly outlined the reasons for treating insiders and outsiders differently in the Bill's general secrecy offences:

> First, 'Commonwealth officer' doesn't necessarily mean an employee; it may be someone who contracts with government or is employed by a contractor. But someone in that position has a particular duty and obligation that arises from having received sensitive information. An outsider doesn't necessarily have that duty. … The second reason is a practical one. In the Commonwealth Public Service, even though there might be cause for improvement and we think it should be improved, we have a Public Interest Disclosure Scheme that applies to officers who work in the Commonwealth. That doesn't apply to outsiders. … If you criminalise the position of outsiders, they don't necessarily have access to the disclosure mechanisms that are available to laypeople. The third thing is that, if an outsider has access to information that they should not have access to, either they have done something that they shouldn't have elsewhere in the law—in which case, that is the appropriate offence to tackle that—or someone has given it to them and the question then is: has that person then done something that they shouldn't have done? But the position of the outsider is not what these secrecy offences ought to be targeted to.[115]

4.114 The Law Council of Australia submitted that the application of the secrecy provisions to outsiders was 'not adequately justified' and that they 'do not contain adequate safeguards for protecting the rights of outsiders'. The Law Council recommended the provisions be redrafted to treat insiders and outsiders separately 'to improve the proportionality of the measures'.[116]

4.115 In response to these concerns, the Attorney-General's Department noted:

---

114 Independent National Security Legislation Monitor, *Report on the impact on journalists of section 35P of the ASIO Act*, October 2015, p. 23.

115 Dr Aruna Sathanapally, Director, Legal Advocacy, Human Rights Law Centre, *Committee Hansard*, Canberra, 30 January 2018, p. 60.

116 Law Council of Australia, *Submission 5*, pp. 55, 57.

> Protecting Australia from espionage and foreign interference relies heavily on having strong protections for information, especially where disclosure causes harm to an essential public interest. The unauthorised disclosure or use of certain information can prejudice national security and defence or our relationships with foreign countries.
>
> In the same way as any person can commit espionage, any person can threaten Australia's safety, security and stability through the unauthorised disclosure of harmful information.[117]

Definition of 'Commonwealth officer'

4.116 'Commonwealth officer' is defined in proposed section 121.1 to mean any of the following:

> (a) an APS employee;
>
> (b) an individual appointed or employed by the Commonwealth otherwise than under the *Public Service Act 1999*;
>
> (c) a member of the Australian Defence Force;
>
> (d) a member or special member of the Australian Federal Police;
>
> (e) an officer or employee of a Commonwealth authority;
>
> (f) an individual who is a contracted service provider for a Commonwealth contract;
>
> (g) an individual who is an officer or employee of a contracted service provider for a Commonwealth contract and who provides services for the purposes (whether direct or indirect) of the Commonwealth contract.

4.117 The Law Council of Australia noted that the proposed definition of 'Commonwealth officer' does not include the Governor-General or parliamentarians who are not appointed to roles of a Minister of State or Parliamentary Secretaries. The Law Council recommended that the Committee consider whether the definition should be expanded to include the Governor-General, as was recommended by the ALRC. It argued that, as the head of state, the Governor-General 'should arguably meet higher levels of accountability to the Australian people'.[118]

---

117 Attorney-General's Department, *Submission 5*, pp. 17-18.

118 Law Council of Australia, *Submission 5*, pp. 65-66.

4.118 The Attorney-General's Department confirmed that expanding the definition of 'Commonwealth officer' to include the Governor-General would, mean: firstly, that information made or obtained by the Governor-General would be subject to the offences in sections 122.1 and 122.2; and, secondly, that the Governor-General could commit the offence at section 122.4 by communicating information that he or she was under a duty not to disclose.[119]

4.119 Including the Governor-General in the definition of 'Commonwealth officer' would also make the defence in section 122.5(1) available for any dealings the Governor-General may have with Commonwealth information.

Government proposed amendments – separate offences for 'outsiders'

4.120 On 13 February 2018, the Attorney-General's Department advised the Committee that it had been asked by the Attorney-General to progress a number of changes to the general secrecy offences in Schedule 2 to the Bill. These amendments included 'creating separate offences that apply to non-Commonwealth officers that are narrower in scope than those applying to Commonwealth officers and only apply to the most serious and dangerous conduct'. The Committee received draft amendments to this effect from the Attorney-General on 5 March 2018.[120] The proposed amendments included:

- limiting the offences in proposed sections 122.1 and 122.2, and the aggravated offences in proposed section 122.3, to information made or obtained by a person by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity.
- creating two separate offences, in proposed section 122.4A, in relation to non-Commonwealth officers. The separate offences would be limited to communications, or other dealings, in which
    i. the information has a security classification of SECRET or TOP SECRET,
    ii. the conduct damages the security or defence of Australia,
    iii. the conduct interferes with or prejudices the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth,

---

119 Attorney-General's Department, *Submission 6.1*, p. 21.

120 Attorney-General, *Submissions 40 and 40.1*.

iv. the conduct harms or prejudices the health or safety of the Australian public or a section of the Australian public.

- reducing the maximum penalties for the offences for non-Commonwealth officers from 15 years to 10 years imprisonment for communications, and from five years to three years imprisonment for other dealings.
- providing that, in proceedings for an offence against the proposed new section 122.4A, the prosecution is not required to prove the identity of the Commonwealth officer (or person otherwise engaged by a Commonwealth entity) who initially provided the information.

4.121 The Attorney-General also proposed excluding officers or employees of, or persons engaged by, the Australian Broadcasting Corporation and the Special Broadcasting Services Corporation from the definition of 'Commonwealth Officer'. The Attorney-General explained that this amendment 'appropriately recognises that members of these organisations, while being public employees, are engaged primarily in journalism and communications activities'.[121]

4.122 The proposed amendments were generally supported by participants in the inquiry.[122] The Law Council of Australia, for example, submitted that the proposed amendments, in principle 'are to be commended as a significant improvement' to the secrecy offences. However, the Law Council noted its concern about the severity of the 15 year maximum penalty that would continue to apply in relation to Commonwealth officers.[123]

4.123 The Human Rights Law Centre welcomed the proposal to limit proposed sections 122.1 to 122.3 to Commonwealth officers, and noted that—with the exception of the paragraphs relying on security classifications—new section 122.4A adopts harm as an essential element of each offence. The Centre, however, expressed the following concerns about the new offence:

> [P]roposed new section 122.4A does not capture an essential element of any secrecy offence that applies to outsiders, being either that the outsider was provided the information on a confidential basis, or that the outsider knew or was reckless as to the fact that the information was disclosed to them in breach of a secrecy offence.

---

121 Attorney-General , *Submission 40*, p. 2.

122 Law Council of Australia, *Submission 5.1*, p. 4; Human Rights Law Centre, *Submission 11*, p. 2; Joint councils for civil liberties, *Submission 31*, p. 9.

123 Law Council of Australia, *Submission 5.1*, p. 4.

> Moreover … the proposed new offence is not limited to disclosure but extends to 'dealing' with information, which includes receipt, possession or making a record. Therefore, it appears that, even with these proposed amendments, the Bill would criminalise innocent receipt of information by a non-Commonwealth officer, if the information has a security classification of secret or above.[124]

4.124 At a public hearing, the Centre further commented that

> if you are then going to put criminal offences on anyone—the ordinary person or the person who is engaged in some function that isn't part of government—for essentially dealing with, sharing or disclosing information, there needs to be some duty or reason why the person could not deal with that information freely.[125]

4.125 The Centre referred the Committee to the ALRC's 'clear guidance' with respect to the principles to guide the creation of any secrecy offence applying to non-Commonwealth officers, and encouraged the Committee to view new section 122.4A as 'essentially the general secrecy offence recommended by the ALRC to apply to Commonwealth officers'.[126]

Consistency with freedom of information laws

4.126 Under the *Freedom of Information Act 1982* (the FOI Act), every person has a legally enforceable right to obtain access to a document of an agency or an official document of a Minister, other than exempt documents.[127] Exempt documents include documents affecting national security, defence or international relations; Cabinet documents; documents affecting enforcement of law and protection of public safety; and a range of other documents. The Act also provides for a range of public interest conditional exemptions.[128]

4.127 The Human Rights Law Centre submitted that breadth of the proposed new secrecy offences is such that 'they criminalise the disclosure of information

---

124 Human Rights Law Centre, *Submission 11*, p. 2.

125 Dr Aruna Sathanapally, Director of Legal Advocacy, Human Rights Law Centre, *Committee Hansard*, Melbourne, 16 March 2018, p. 21.

126 Human Rights Law Centre, *Submission 11*, p. 2.

127 *Freedom of Information Act 1982*, section 11.

128 *Freedom of Information Act 1982*, Part IV.

to which Australians have a right to access under the FOI Act'.[129] The Centre provided several examples to demonstrate this point:

- New section 122.1 criminalises disclosure of "information relating to the operations, capabilities or technologies of, or methods or sources used by, a domestic or foreign law enforcement agency," whereas the FOI Act only exempts documents whose disclosure would or could reasonably be expected to "disclose lawful methods or procedures for preventing, detecting, investigating, or dealing with matters arising out of, breaches or evasions of the law the disclosure of which would, or would be reasonably likely to, prejudice the effectiveness of those methods or procedures" or "prejudice the maintenance or enforcement of lawful methods for the protection of public safety". The secrecy offence also extends to foreign law enforcement agencies, whereas the FOI Act exemption does not.
- New section 122.2 extends to information the handling of which would harm or prejudice relations between the Commonwealth and a State or Territory, whereas under the FOI Act, a document the disclosure of which would, or could reasonably be expected to, cause damage to relations between the Commonwealth and a State is only conditionally exempt from release, meaning that it is only exempt if its release would, on balance, be contrary to the public interest (see ss 11A and 47B of the FOI Act). New section 122.2 contains no such public interest test.
- The FOI Act provides no exemption for security classified information … Rather than merely relying on security classifications or other protective markings, the FOI decision-maker has to independently turn their mind to the question of whether a document's disclosure would cause damage to specified public interests. As such, persons disclosing security classified or marked "for Australian Eyes Only" information could be caught under the proposed offences, notwithstanding that the information could be legally obtained under the FOI Act.[130]

4.128 The Department responded to the Centre's concern as follows:

---

129 Human Rights Law Centre, *Submission 11*, p. 15.

130 Human Rights Law Centre, *Submission 11*, pp. 15–16.

> The secrecy offences are subject to a defence for persons acting within their powers, functions and duties as a Commonwealth officer. This would include release of information under freedom of information laws.[131]

4.129 Following release of the government's proposed amendments to the definition of 'inherently harmful information' (discussed above), the Human Rights Law Centre commented that paragraph (e) of the definition 'remains inconsistent with the principles in the FOI Act with respect to domestic law enforcement agencies'.[132]

Replication of section 70 of the Crimes Act

4.130 Section 70 of the Crimes Act currently consists of the following offences, punishable by imprisonment for up to two years.

> (1) A person who, being a Commonwealth officer, publishes or communicates, except to some person to whom he or she is authorized to publish or communicate it, any fact or document which comes to his or her knowledge, or into his or her possession, by virtue of being a Commonwealth officer, and which it is his or her duty not to disclose, commits an offence.
>
> (2) A person who, having been a Commonwealth officer, publishes or communicates, without lawful authority or excuse (proof whereof shall lie upon him or her), any fact or document which came to his or her knowledge, or into his or her possession, by virtue of having been a Commonwealth officer, and which, at the time when he or she ceased to be a Commonwealth officer, it was his or her duty not to disclose, commits an offence.

4.131 The Explanatory Memorandum provides the following overview of deficiencies in the existing offence:

> The drafting of section 70 is outdated and complicated, resulting in a lack of clarity about the scope of the offence. For example, section 70 will be enlivened where a Commonwealth official is subject to a duty of non-disclosure arising elsewhere. It is well-established that a statutory duty of non-disclosure may enliven the offence. Comparatively, it remains unresolved whether a duty at common law or in equity would be a relevant duty for the purposes of the offence. Similarly, the offence requires the disclosure of a 'fact or document'. The application of the offence to the disclosure of factual information or documents is well-established, however there is some uncertainty about the

131 Attorney-General's Department, *Submission 6.1*, p. 38.

132 Human Rights Law Centre, *Submission 11.2*, p. 5.

> application of the offence to the disclosure by a Commonwealth official of matters of opinion or advice that are not factual in nature in a non-documentary form.[133]

4.132 The Explanatory Memorandum notes that there have been calls for 'significant reforms' to the existing Crimes Act secrecy offences 'for many years'. In particular, the Explanatory Memorandum notes the ALRC's report *Secrecy Laws and Open Government in Australia* (see above). In that report, the ALRC summarised its concerns with the section 70 offences as follows:

> There are real concerns about the way that s 70 of the Crimes Act is framed—in particular, the need to establish a 'duty not to disclose' independently of the offence provision. In the ALRC's view, where it is the Australian Parliament's intention to impose criminal sanctions for disclosure of Commonwealth information, this should be done in a single offence provision so that there is a clear and certain link between the conduct being criminalised and the criminal penalty imposed.[134]
>
> …
>
> Despite the views of some stakeholders that s 70 of the Crimes Act is relatively straightforward to enforce and should be retained, the 'catch-all' nature of the provision is seriously out of step with public policy developments in Australia and internationally … there is also an argument to be made that a law that imposes criminal liability on all Commonwealth officers for unauthorised disclosure of any official information—and does not differentiate between the types of information protected or the consequences of disclosure—does not sit comfortably with the implied constitutional freedom of communication about government and political matters, or with Australia's international human rights obligations.[135]

4.133 The ALRC recommended that section 70 [and the official secrets offence in section 79(3)] be repealed and replaced by new offences in the *Criminal Code*.[136]

---

133 Explanatory Memorandum, p. 221.

134 Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, Report 112, December 2009, pp. 122-123.

135 Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, Report 112, December 2009, p. 137.

136 Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, Report 112, December 2009, p. 170.

4.134 In accordance with the ALRC's recommendation, the Bill proposes to repeal section 70 from the Crimes Act. However, the Bill effectively replicates the offences in section 70 (albeit in a modernised form) in new proposed section 122.4 of the *Criminal Code*.

4.135 Some participants in the inquiry raised concerns about the Bill's replacement of section 70 with similar provisions in proposed section 122.4. For example, Dr Luke Beck of Monash University questioned why the offence was included in a national security Bill at all:

> Clause 122.4 captures public service leaks on any subject matter and regardless of the implications, if any, of the leak. The provision seems to be a catch-all public service leaks offence. The provision does not pursue any national security purpose. It is not readily apparent why such a provision is found in a Bill that is ostensibly about "national security", "espionage" and "foreign interference".[137]

4.136 The Human Rights Law Centre submitted that proposed section 122.4 'replicates the recognised flaws' in section 70, 'not only in lacking any requirement that the disclosure result in harm', but also:

- Both [section] 70 and new section 122.4 apply to any information a Commonwealth officer learns in their job regardless of its nature or sensitivity (provided they have a duty not to disclose it) … [and]
- Like [section] 70, new section 122.4 applies where a person had a "duty not to disclose" the relevant information, but does not provide that duty itself, or even the Acts in which those duties are contained. Instead, the duty must be found elsewhere.[138]

4.137 The Centre concluded that it was 'difficult to see the necessity of new section 122.4 in light of the other offences introduced by the Bill, which cover a wide array of conduct'.[139] The Centre commented:

> The entire ALRC report was directed to why sections 70 and 79 of the Crimes Act needed to be repealed and what needed to replace them, yet this bill would make section 70 an enduring feature of Commonwealth law with no

---

137 Dr Luke Beck, Associate Professor, Faculty of Law, Monash University, *Submission 41*, p. 1.

138 Human Rights Law Centre, *Submission 11*, p. 13.

139 Human Rights Law Centre, *Submission 11*, p. 13.

> concrete timetable for repeal. That would be a real disappointment for necessary law reform in Australia.[140]

4.138 The Explanatory Memorandum provides the following rationale for the inclusion of proposed section 122.4 in the Bill:

> At present, many Acts and Regulations impose duties of non-disclosure on Commonwealth officers that enliven the offence in section 70 of the Crimes Act. If section 70 were repealed without replacement, those duties would lose their criminal enforceability, potentially undermining the protection of information that should appropriately be protected.
>
> The offence in section 122.4 is intended to preserve the operation of those specific secrecy frameworks, until such time as each duty can be reviewed to determine whether it should be converted into a stand-alone specific secrecy offence, or whether criminal liability should be removed. Given the number and diversity of such duties, this review will be conducted as each duty is next considered, rather than within a specific period of time. Accordingly, this offence is not subject to a sunset provision.[141]

4.139 The joint media organisations recommended that the Committee consider a sunset provision 'so that the "review" is not allowed to go on indefinitely'.[142]

4.140 In its report, the ALRC identified 23 provisions that were not themselves criminal , but may give rise to a 'duty not to disclose' for the purpose of section 70. However, the ALRC also noted there was a 'lack of clarity' as to which duties may give rise to criminal liability under section 70.[143]

Freedom of expression and political communication

4.141 Several submissions raised concerns about the impact of the proposed secrecy offences on the right to freedom of expression and the implied constitutional right to freedom of political communication.[144] The nature of

---

140 Dr Aruna Sathanapally, Director of Legal Advocacy, Human Rights Law Centre, *Committee Hansard*, Melbourne, 16 March 2018, p. 20.

141 Explanatory Memorandum, p. 272.

142 Joint media organisations, *Submission 9*, p. 4.

143 Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, Report 112, December 2009, p. 126 and Appendix 4.

144 Law Council of Australia, *Submission 5*, pp. 55–56, 67; Human Rights Law Centre, *Submission 11*, pp. 3–5; Australian Human Rights Commission, *Submission 17*, p. 5; Centre for Media Transition, University of Technology, Sydney, *Submission 23*, p. 2; United Nations Special Rapporteurs, *Submission 30*, p. 5; Joint councils for civil liberties, *Submission 31*, p. 6.

these rights and the general concerns raised by submitters about the Bill's impact on these rights are discussed in Chapter 3.

4.142 The Australian Human Rights Commission submitted that the Bill should not be passed 'unless and until the secrecy offences in Schedule 2 are amended to ensure they are necessary and proportionate to achieve their objective, and are consistent with the freedom of expression'.[145] Specifically, the Commission was concerned that the secrecy offences:

- do not, for the most part, distinguish between conduct engaged in by 'insiders' and by 'outsiders',
- are not limited to prohibiting disclosures that are shown to damage the interests of the Commonwealth,
- contain inappropriate strict liability provisions,
- do not contain adequate defences.[146]

4.143 Dr Luke Beck, an Associate Professor of Constitutional Law, submitted that he 'would not be confident of the constitutional validity' of the offences in proposed section 122.2:

> To avoid violating the implied freedom of political communication, such a burden must be reasonably capable of being seen as appropriate and adapted to achieving its legitimate purpose. Assuming the prevention of harm to Australia's interests is the purpose of the provision, clause 122.2 appears to fail this test. The provision criminalises the communication of information (i) in respect of which of there is no other legal duty not to disclose and (ii) which concerns not only serious matters relating to national security but also minor matters that are merely administratively or politically inconvenient or embarrassing rather than genuinely harmful.
>
> The provision prohibits communications of information that do not genuinely harm Australia's interests. The offence applies to more conduct than is reasonably necessary to achieve the purpose of preventing harm to Australia's interests. Alternative, less restrictive means of achieving that purpose exist. To be compatible with the implied freedom of political communication the definition of 'cause harm to Australia's interests' needs to be more carefully calibrated to apply only to communications that would genuinely harm Australia's interests.[147]

---

145 Australian Human Rights Commission, *Submission 17*, p. 5.

146 Australian Human Rights Commission, *Submission 17*, pp. 4–5.

147 Dr Luke Beck, Associate Professor, Faculty of Law, Monash University, *Submission 41*, p. 1.

4.144 The Law Council of Australia similarly considered that a constitutional challenge to the proposed secrecy provisions on the grounds that they breach the implied right to freedom of political communication 'may be likely'.[148]

4.145 The Committee received a joint submission from the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, and Special Rapporteur on the situation of human rights defenders. The Special Rapporteurs drew attention to the Australian Government's obligations under Article 19 of the International Covenant on Civil and Political Rights with respect to freedom of opinion, and submitted that they were 'gravely concerned' that the Bill may violate those obligations.[149]

4.146 The Special Rapporteurs were particularly concerned about the Bill's provisions regarding 'inherently harmful information' (including the breadth of definitions and prohibited conduct, and the lack of harm and knowledge requirements), the breadth of the definition of what constitutes 'harm to Australia's interests', and limitations in the defences available to whistleblowers and journalists.[150] The Special Rapporteurs submitted:

> We are concerned that the cumulative effect of these restrictions, coupled with the lack of meaningful defenses, will disproportionately restrict disclosures of government related information that is nevertheless in the public interest, particularly disclosures that draw critical public scrutiny to government fraud, waste, and abuse.
>
> We are particularly concerned that these restrictions will disproportionately chill the work of media outlets and journalists, particularly those focused on reporting or investigating government affairs. The lack of clarity concerning these restrictions, coupled with the extreme penalties, may also create an environment that unduly deters and penalizes whistleblowers and the reporting of government wrongdoing more generally.[151]

---

148 Law Council of Australia, *Submission 5*, p. 67.

149 United Nations Special Rapporteurs, *Submission 30*, pp. 2–4, 5.

150 United Nations Special Rapporteurs, *Submission 30*, pp. 5–8.

151 United Nations Special Rapporteurs, *Submission 30*, pp. 8–9.

4.147 The Attorney-General's Department addressed in its submission the need to balance national security concerns with freedom of speech and the implied freedom of political communication:

> 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'.
>
> 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.[152]

4.148 The Department advised that it had considered the implied right to freedom of communication and 'is confident that the offences in the Bill do not infringe on the implied freedom'.[153]

Committee comment

4.149 The Committee recognises that strong measures to protect sensitive Commonwealth information are an essential part of Australia's legal framework. In certain circumstances, the unauthorised disclosure of information has the potential to cause substantial harm to Australia's interests, including harm to Australia's long-term security and defence, and harm to the personal safety of individuals.

4.150 The Committee also recognises that the proposed secrecy offences in Schedule 2 to the Bill are of significant interest to the Australian community. While there appears to be general support for reforming the existing secrecy laws in the Crimes Act, there is concern that the Bill as drafted could

---

152 Attorney-General's Department, *Submission 6*, pp. 32–33.

153 Attorney-General's Department, *Submission 6.1*, p. 74.

criminalise too broad a range of conduct and contains inadequate protections for freedom of expression.

4.151 The Committee therefore welcomes the Attorney-General's proposed amendments. The Committee addresses these amendments and a range of other proposed amendments in the discussion below.

Unsolicited receipt of information

4.152 The Committee notes that, in line with the advice of operational agencies, the secrecy offences in the Bill are deliberately broad in order to capture a range of dealings with information that fall short of communication or disclosure. This includes receiving, obtaining, collecting, possessing, making a record of, and copying information. The Committee notes that, in certain circumstances, such activities may be preparatory to the unauthorised disclosure of sensitive information, and considers it appropriate that the secrecy provisions capture this conduct.

4.153 The Committee acknowledges concerns expressed by some participants in the inquiry that, due to the broad definition of 'deals with', a person could commit a secrecy offence simply by receiving certain information without being aware of the nature of that information. These concerns particularly apply in relation to security classified information and other 'inherently harmful information' under proposed section 122.1, and the proposed new section 122.4A. However, the Committee notes that, due to the default application of fault elements under the *Criminal Code*, in order for a person to be found guilty of one of these offences, a prosecution would need to prove beyond reasonable doubt that the person

- *intentionally* dealt with (i.e. received, possessed, collected, etc.) the relevant information, and
- was *reckless* as to the nature of that information—that is, in the case of security classified information, the person would need to be aware that there is a substantial risk that the information he or she intentionally received was classified, and that having regard to the circumstances known to him or her, it was unjustifiable to take that risk.

4.154 The Committee accepts the views of participants that the operation of these fault elements is not clear on the face of the Bill, and recommends that the Bill be amended to remedy this.

4.155 The Committee also notes that there are a range of circumstances where a person could intentionally receive, or be in the possession of, 'inherently

harmful information' for innocuous reasons. The Committee considers it important that the defences in proposed section 122.5, discussed in the next chapter, be sufficiently robust to respond to such circumstances.

Recommendation 14

4.156 The Committee recommends that the Bill include a note making explicit that the secrecy offences relating to security classified information and other 'inherently harmful information' will only apply where a person intentionally deals with the relevant information, and where the person is reckless as to the nature of that information.

'Inherently harmful information'

4.157 The Committee accepts the proposition that there are certain categories of information that, if inappropriately handled, are likely to cause substantial harm to Australia's essential interests. This includes highly classified information, information produced or obtained by intelligence agencies, and sensitive information relating to the operations, capabilities, methods and sources used by law enforcement agencies.

4.158 The Committee welcomes the Attorney-General's proposed amendments to narrow the scope of the definition of 'inherently harmful information', including by removing paragraph (d)—information that was provided to the Commonwealth 'in order to comply with an obligation under a law or otherwise by compulsion of law'. This amendment will remove from the scope of the offences a range of information that, while potentially sensitive, may not be considered 'inherently harmful' enough to warrant inclusion in the general secrecy offences.

4.159 Also in the definition of 'inherently harmful information' is information the communication of which would, or could reasonably be expected to, damage the security or defence of Australia (paragraph (b)). However, noting that the wording of this paragraph effectively includes a harm-based test, the Committee agrees with the suggestion that it would be more coherent for it to be placed in the definition of 'cause harm to Australia's interests'.[154]

---

[154] The Committee notes that including harm to Australia's security or defence within the definition of 'cause harm to Australia's interests' would have the additional advantage of enabling the defence at section 122.5(8) (discussed in the next chapter) to be simplified. That is, the

Recommendation 15

4.160 The Committee recommends that the Attorney-General's proposed amendments to narrow the scope of the offences at proposed section 122.1 in relation to 'inherently harmful information' be implemented. This includes removing paragraph (d) from the definition of 'inherently harmful information', removing strict liability from elements of the offences, and limiting the offences to Commonwealth officers.

Recommendation 16

4.161 The Committee recommends that the Bill be amended to move paragraph (b)—information the communication of which would, or could be reasonably expected to, damage the security or defence of Australia—from the definition of 'inherently harmful information' into the definition of 'cause harm to Australia's interests' in proposed section 121.1.

'Cause harm to Australia's interests'

4.162 The Committee also welcomes the Attorney-General's proposed amendments to narrow the scope of the definition of 'cause harm to Australia's interests', including by removing contraventions of civil penalty provisions, international relations (other than in relation to information communicated in confidence) and Commonwealth–State/Territory relations from the definition. These amendments will help ensure the offences are more appropriately targeted towards the most harmful conduct.

4.163 The Committee notes that dealing with information in a way that interferes with or prejudices the performance of the AFP's functions under proceeds of crime legislation remains within the definition of 'cause harm to Australia's interests'. The Committee agrees with the Attorney-General's Department that there is an essential public interest in strong action to confiscate proceeds of crime, and supports its continued inclusion in the scope of the offences.

4.164 The Committee also notes concerns expressed by the Law Council of Australia about the breadth of the phrase 'interfere with' in relation to the prevention, detection, investigation, prosecution and punishment of criminal offences, and in relation to certain AFP functions including

---

requirement at 122.5(8)(2) for a person to believe that the communication will not cause harm to 'the security or defence of Australia' would no longer be necessary.

proceeds of crime. Similar wording is included in the terms of the Attorney-General's proposed new offence for non-Commonwealth officers (section 122.4A), albeit limited to criminal offences. While the Committee is concerned to ensure that criticism of police, security or prosecution officials who have acted improperly or negligently is protected, the Committee also notes the risks associated with limiting the ability of police to act when a person's conduct is interfering with, but has not yet prejudiced, a criminal investigation. The Committee considers that the most appropriate way to balance these objectives is to ensure that the defences available in the legislation cover the reporting of corrupt behaviour and maladministration by the authorities. This is discussed further in the next chapter.

Recommendation 17

4.165 The Committee recommends that the Attorney-General's proposed amendments to narrow the scope of the offences at proposed section 122.2 in relation to conduct causing harm to Australia's interests be implemented. This includes removing paragraphs (a)(i), (d) and (e) from the definition of 'cause harm to Australia's interests', clarifying that paragraph (f) applies to the health or safety of the *Australian* public, or a section of the *Australian* public, and limiting the offences to Commonwealth officers.

Proper place of custody offences

4.166 The Committee notes that the intention of the 'proper place of custody' offences at proposed subsections 122.1(3) and 122.2(3) is that they will apply to contraventions of existing requirements for Commonwealth departments and agencies to handle classified information in accordance with the Commonwealth *Protective Security Policy Framework*. The Committee notes that the framework is proposed to be incorporated by reference into regulations that define the term 'proper place of custody' for the purpose of these offences.[155] To ensure that the law is able to be readily understood, the Committee considers it appropriate that any material incorporated into these regulations should be required to be publicly available.

[155] Explanatory Memorandum, p. 234.

Recommendation 18

4.167 The Committee recommends that the Bill be amended to require that any material incorporated into regulations for the purpose of the definition of 'proper place of custody' at proposed section 121.2 be publicly available.

'Lawful direction' offences

4.168 Proposed subsections 122.1(4) and 122.2(4) make it an offence for a person to fail to comply with a lawful direction regarding the retention, use or disposal of certain sensitive information. Noting the potential for serious harm to result from the mishandling of sensitive information, the Committee supports in principle this conduct being the basis of a criminal offence.

4.169 However, the Committee agrees with the Inspector-General of Intelligence and Security that it would not be appropriate for the offence concerning 'inherently harmful information' to extend to lawful directions that have no bearing upon the protection of the security of that information. The Committee therefore supports the suggestion that further statutory parameters be included in the Bill to more narrowly target the scope of the offence at proposed subsection 122.1(4).

Recommendation 19

4.170 The Committee recommends that the Bill be amended to limit the secrecy offence at proposed section 122.1(4), in relation to failing to comply with a lawful direction, to directions that have been issued for the purpose of protecting the security of the 'inherently harmful information' against unauthorised access or disclosure.

Aggravated offences

4.171 The Committee agrees in principle that there will be circumstances in which a person has a higher degree of culpability with respect to the proposed secrecy offences that will warrant aggravated penalties being available. This includes circumstances where the information that a person deals with or communicates is code worded, consists of five or more records, or where the person alters a record to remove or conceal a security classification.

4.172 The Committee supports the Attorney-General's proposed amendment to remove the aggravating factor in subparagraph 122.3(1)(b)(i). As the definition of 'security classification' is now proposed to be limited to

classifications of secret or above, it would not be appropriate for such information to be the subject of an aggravating factor.

4.173 The Committee holds concerns, however, about the scope of the aggravating factor in subparagraph 122.3(1)(b)(v)—that at the time the person committed the underlying offence, the person held an Australian Government security clearance. The Explanatory Memorandum states that 'Australian Government security clearance' is intended to capture all security clearances granted by the Australian Government Security Vetting Agency (AGSVA) or another government agency conducting and issuing security clearances under the Protective Security Policy Framework. This would include clearances from 'Baseline' up to 'Top Secret Positive Vetting' levels.[156]

4.174 Under the amendments proposed by the Attorney-General, the offences in sections 122.1 and 122.2 will only apply to Commonwealth Officers. While the Committee accepts that persons holding higher level clearances have additional responsibilities, the Committee considers that the holding of a Baseline clearance is not sufficiently differentiated from non-clearance holders to justify an aggravated penalty. Baseline security clearances are the lowest level granted by AGSVA, and enable a holder to access information up to 'Protected'—the lowest security classification. As at September 2017, there were 114 101 active Baseline clearances managed by AGSVA,[157] with many government entities requiring all employees to hold a Baseline clearance in order to access their records management system.[158] A Baseline clearance will not be sufficient for a person to access 'security classified information'—that is, information with a classification of SECRET or above—under the revised definition in the Bill. A clearance of 'Negative Vetting 1' would be the minimum required to access such information. The Committee therefore considers it would be more appropriate to limit the aggravating factor to clearances of Negative Vetting 1 (or equivalent) and above.

---

156 Explanatory Memorandum, p. 271

157 Australian National Audit Office, *Mitigating Insider Threats through Personnel Security*, *Report No. 38 of 2017–18*, May 2018, pp. 17. There were additionally 114 994 active Protected, Highly Protected, Confidential, Restricted and Entry clearances managed by AGSVA that were granted prior to the security clearance levels being changed in 2010.

158 Australian National Audit Office, *Central Administration of Security Vetting, Report No. 45 of 2014-2015*, June 2015, p. 103.

Recommendation 20

4.175 The Committee recommends that the Bill be amended to limit the aggravating factor at subparagraph 122.3(1)(b)(v), in relation to the proposed secrecy offences for Commonwealth officers, to persons holding an Australian Government security clearance that allows the person to access information with a classification of SECRET or above.

Application to non-Commonwealth officers

4.176 One of the recurring criticisms of the Bill raised in submissions to the inquiry was that the offences apply equally to both Commonwealth officers and to all other persons. The Committee agrees with these participants that Commonwealth officers have greater obligations than other persons in respect to the confidentiality of Commonwealth information.

4.177 The Committee therefore strongly supports the Attorney-General's proposal for separate secrecy offences, narrower in their range of conduct captured, to be established for non-Commonwealth officers.

4.178 While the Committee notes that the proposed new offences for non-Commonwealth officers do not fully replicate the model proposed by the Australian Law Reform Commission, the Committee notes that the offences are appropriately limited to highly classified information and conduct that results in, or is likely to result in, harm to essential public interests.

Recommendation 21

4.179 The Committee recommends that the Attorney-General's proposed amendments, to create separate secrecy offences that apply to non-Commonwealth officers that are narrower in scope than those applying to Commonwealth officers, be implemented.

Consistency with freedom of information laws

4.180 The Committee notes evidence that the proposed secrecy offences may prohibit dealing with or communicating information that would otherwise be accessible to Australians under the freedom of information legislation. By narrowing the definitions of 'inherently harmful information' and 'causes harm to Australia's interests', the Attorney-General's proposed amendments would reduce the level of inconsistency between the two regimes. However, the Committee notes the view of one submitter that there continues to be

differences in respect of information relating to domestic and foreign law enforcement agencies.

4.181 The Committee notes there is an important difference between information that a person may request access to under the Freedom of Information Act, and information that would properly be disclosed under that Act. It is open to a person to request almost any information held by a government agency, unless the information or agency is covered by section 7 of the Act (Exemption of certain persons and bodies). However, Part IV of the Act contains a range of exemptions and conditional exemptions, which then narrow the scope of information that may in fact be released. The existence of these exemptions and conditional exemptions reflects an important balance between open government, and the need for some information to remain properly confidential.

4.182 The Committee notes that the defence in subsection 122.5(1) would cover the provision of information by a Commonwealth officer to an applicant under the FOI Act process. That is to say, the Bill would not appear to impede the proper operation of the FOI Act process. Similarly, the defence in subsection 122.5(2) is intended to extend to 'information members of the public are entitled to request access to, even if no members of the category do request access to it'. This would presumably include information that has been released to an applicant under the FOI Act, and which would therefore be available on request from the relevant department or agency.

Recommendation 22

4.183 The Committee recommends that the Bill be amended to make clear the effect of the defences in subsections 122.5(1) and (2) in relation to the *Freedom of Information Act 1982*.

Section 122.4 – replication of section 70 of the Crimes Act

4.184 The Committee notes that proposed section 122.4 largely replicates the existing secrecy offences proposed to be removed from in section 70 of the Crimes Act. This offence has been included in the Bill to 'preserve the operation of' other Acts and Regulations that impose duties of non-disclosure on Commonwealth officers 'until such time as each duty can be

reviewed to determine whether it should be converted into a stand-alone specific secrecy offence, or whether criminal liability should be removed'.[159]

4.185 However, given the well-documented problems with the existing section 70 offence that are replicated in proposed section 122.4, and noting the already broad scope of the new secrecy offences in proposed sections 122.1 and 122.2, the Committee considers it would be appropriate to put an outer limit on this period of review. This will ensure the provision is in fact repealed once enough time has elapsed for the dependent laws to be reviewed.

4.186 The Committee notes that the ALRC, in its comprehensive report on *Secrecy Laws and Open Government in Australia*, was only able to identify 23 duties likely to give rise to criminal liability under section 70.[160] The Committee considers a five-year sunset period on section 122.4 would allow sufficient time for the Attorney-General's Department to review each of those duties and to determine whether there is an ongoing need to enforce them with specific criminal sanctions.

Recommendation 23

4.187 The Committee recommends that the Bill be amended to apply a sunset period of five years to proposed section 122.4 ('Unauthorised disclosure of information by current and former Commonwealth officers etc.').

Review of specific secrecy offences in other legislation

4.188 The Committee also notes the array of specific secrecy offences in other legislation that will continue to exist once the proposed new general offences have been added to the *Criminal Code*. The Committee notes the findings in the ALRC's report as to the role of these offences—of which the ALRC identified more than 500—and the set of principles that should guide the creation of any new offences and the review of existing offences.[161] It is likely that many of these existing offences will no longer be required, or will require amendment, with the passage of the new offences.

---

159 Explanatory Memorandum, p. 272.

160 Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, Report 112, December 2009, p. 126 and Appendix 4.

161 Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, Report 112, December 2009, Chapter 9 and Appendix 4.

4.189 In addition to reviewing the provisions that will be enlivened by proposed section 122.4, the Committee therefore recommends that these broader secrecy provisions be reviewed as soon as possible to determine whether they are still required with the enactment of the proposed offences in Schedule 2, or whether amendments are required. The ALRC's guidance should be taken into account in this review.

Recommendation 24

4.190 The Committee recommends that, following the passage of the general secrecy offences in Schedule 2 to the Bill, the Attorney-General initiate a review of existing secrecy offences contained in other legislation, taking into account the set of principles contained in the Australia Law Reform Commission's report, *Secrecy Laws and Open Government in Australia*.

5. Secrecy offences - defences and other matters

5.1 This chapter considers

- evidence concerning the offence-specific defences available in relation to the secrecy offences in Schedule 2 to the Bill,
- other matters concerning the secrecy provisions, including interactions with other legislation, the Attorney-General's consent to institute proceedings, penalties and consequential amendments, and
- the Committee's conclusions in relation to these matters.

Defences

5.2 In addition to the range of general defences available under Part 2.3 of the *Criminal Code*, the Bill's secrecy provisions contains a range of offence-specific defences, for which the defendant bears an evidential burden. A broad range of issues were raised with the Committee about the scope and clarity of these defences, and their application in a range of contexts.

Official duties – subsection 122.5(1)

5.3 The defence in proposed section 122.5(1) provides:

> It is a defence to a prosecution for an offence by a person against this Division that:
>
> (a) the person was exercising a power, or performing a function or duty, in the person's capacity as a Commonwealth officer or a person who is otherwise engaged to perform work for a Commonwealth entity; or

(b) the person dealt with, removed or held the information in accordance with an arrangement or agreement to which the Commonwealth or a Commonwealth entity is party and which allows for the exchange of information.

Evidential burden on the defendant

5.4 The effect of placing an evidential burden on the defendant is discussed in general terms in Chapter 3.

5.5 In relation to the proposed secrecy offences, the Commonwealth Ombudsman noted:

> [T]here is a policy question of whether Commonwealth officials should be caught by criminal offences by the mere act of carrying out their duties. An alternative could be for the offence to contain an element to be proved by the prosecution that the person was not acting in the course of their duties.
>
> … Commonwealth Ombudsman staff will need to rely on a defence to a serious offence in order to perform the duties of their role because they will be "dealing with" or "communicating" inherently harmful information.[1]

5.6 The Acting Commonwealth Ombudsman explained how this reversal of the evidential burden may create a 'chilling effect' on agency staff responding to requests for information from the Ombudsman's office:

> We rely on agencies to provide that information for us to deal with complaints and systemic issues, when we request it, in a timely manner so that we can conduct our investigations. So the concern that we are really raising is: the new provisions, or the new offences, may have a chilling effect on agency staff to feel comfortable about responding to those requests for information to our office.[2]

5.7 The IGIS raised similar concerns in her submission, noting that the framing of the provisions in this way 'raises a general question of whether it is appropriate for the criminal law to place individual officers in this position'.[3] At a public hearing, the Deputy IGIS contrasted the Bill to the existing secrecy offences in the *Australian Security Intelligence Organisation Act 1979*

---

1 Commonwealth Ombudsman, *Submission 8*, pp. 3, 4.

2 Ms Jaala Hinchcliffe, Acting Commonwealth Ombudsman, *Committee Hansard*, Canberra, 31 January 2018, p. 5.

3 Inspector-General of Intelligence and Security, *Submission 13*, p. 5.

(ASIO Act) and *Intelligence Services Act 2001*, which were significantly amended in 2014:

> In respect of inspector-general officials, rather than it being a defence to an offence that they were acting in the course of their duties, it's an exception to the offence, which is a subtle but important difference in terms of the evidential onus. In the ASIO Act and the Intelligence Services Act model, the onus is reversed. The onus is on the prosecution to show that they weren't acting in the course of their duties rather than on the official to lead evidence that, because of our secrecy provisions, they may have difficulty in leading.[4]

5.8 Responding to these concerns, the Attorney-General's Department submitted:

> The department considers it appropriate for the defendant to bear an evidential burden for pointing to evidence of how his or her conduct was authorised, either under law or as part of his or her duties. As set out at paragraph 1617 of the Explanatory Memorandum, the imposition of an evidential burden is appropriate because the defendant should be readily able to point to evidence that their conduct was either done in their official capacity as a Commonwealth officer. If this is done, the prosecution must refute the defence beyond reasonable doubt.[5]

5.9 The Committee noted the following view expressed by the ALRC in its 2009 report:

> While framing a provision as a defence, rather than as an exception, does not of itself alter evidential burdens of proof, it may have procedural advantages for a defendant, in that a defendant must wait until the defence case is called before being able to lead evidence to justify his or her conduct.[6]

5.10 However, the Department advised that, after consultation with the Commonwealth Director of Public Prosecutions, it did not agree with the ALRC's view:

> Regardless of whether the provision is framed as an exception or defence, the accused must discharge the evidential burden pursuant to section 13.3 of the Criminal Code. In either circumstance, an accused may do this by relying on

---

4 Mr Jake Blight, Deputy Inspector-General of Intelligence and Security, *Committee Hansard*, Canberra, 31 January 2018, p. 4.

5 Attorney-General's Department, *Submission 6.1*, p. 26.

6 Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, Report 112, December 2009, p. 229.

> matters that form part of the prosecution case or seeking to lead evidence as part of the defence case, to discharge the burden. The question of whether the evidential burden has been satisfied is a question of law, to be decided by a judge. If discharged, the question of whether the prosecution has disproven the defence/exception beyond reasonable doubt is put to a jury.
>
> Neither the department nor the Office of the Commonwealth Director of Public Prosecution is aware of there being a difference in procedure for an exception or a defence.[7]

5.11 The Department added:

> An accused person may, for forensic reasons, wait until the defence case is called before revealing evidence to justify his or her conduct, but they do not have to take that course. An accused person may, and sometimes will, act proactively to advance evidence of a defence in a record of interview, by way of a statement or by supplying evidence to the prosecution in advance of a trial or a prosecution being initiated. This observation applies equally whether the provision is framed as an exception or defence.[8]

5.12 The Department also clarified that, in the case of existing secrecy offences in section 18B (for example) of the ASIO Act, a burden of proof is not placed on the defendant for conduct engaged in in the course of their duties as an ASIO employee or affiliate, because the absence of this circumstance is an element of the offence and must be proved by the prosecution.[9] However, the Department noted that if each of the eight defences (and 20 operative limbs) in proposed section 122.5 were to be similarly reframed as elements

---

7 Attorney-General's Department, *Submission 6.5*, p. 1.

8 Attorney-General's Department, *Submission 6.5*, pp. 1–2.

9 Attorney-General's Department, *Submission 6.5*, pp. 2–3. Section 18A of the ASIO Act makes it an offence for an entrusted person to engage in relevant conduct (copying, transcribing, retaining, removing or otherwise dealing with) concerning ASIO records. It is an element of the offence that 'the relevant conduct was not engaged in by the person (i) as an ASIO employee in the course of the person's duties as an ASIO employee; or (ii) as an ASIO affiliate in accordance with the contract, agreement or other arrangement under which the person is performing functions or services for the Organisation; or (iii) in accordance with a contract, agreement or arrangement the person has entered into with ASIO (other than as an ASIO affiliate); or (iv) acting within the limits of authority conferred on the person by the Director-General; or (v) with the approval of the Director-General, or of a person having the authority of the Director-General to give such an approval'. Similar elements are found in secrecy offences elsewhere in the ASIO Act (sections 18 and 18B) and in the *Intelligence Services Act 2001* in relation to other intelligence agencies.

of the offence, 'the prosecution would need to prove that these circumstances did not exist' before the offence could be proved:

> Proving all of these matters beyond reasonable doubt would be burdensome and costly when compared to the approach taken in the Bill of providing defences for the defendant to raise, as appropriate and as relevant to the individual facts and circumstances of the particular case. It is unlikely that all of these elements will be relevant to each prosecution ….[10]

Application to the Inspector-General of Intelligence and Security

5.13 The IGIS pointed out an unintended consequence, specific to her office, of placing the initial evidentiary burden on the defendant to show that their dealing or communication with information was covered by the defence. Section 34 of the *Inspector-General of Intelligence and Security Act 1986* makes it an offence for the IGIS or her staff to disclose information obtained in the course of their duties to any person, *or to a court*, other than for the performance of functions or duties under that Act or the *Public Interest Disclosure Act 2013*. As a result, the IGIS noted

> In the event that a current or former IGIS official was investigated for, or charged with, one of the proposed offences in Division 122 of the Criminal Code, it would, for all practical purposes, be impossible for them to discharge the evidential burden of proving that the alleged dealing with or communication of information contrary to the proposed offences was undertaken in the course of their duties. Indeed, they would potentially commit an offence under s 34(1) of the IGIS Act by disclosing that information in their defence at trial, or providing it to law enforcement officials investigating the potential commission of an offence under Division 122. Similar difficulties may arise in the investigation or prosecution of a person who made a complaint or disclosure to the IGIS that included 'inherently harmful information'.[11]

5.14 The IGIS suggested that it would be preferable for the elements of the proposed secrecy offences to contain an exclusion of IGIS officials, similar to the existing exclusions in section 18D of the ASIO Act and section 41B of the *Intelligence Services Act 2001*. An IGIS official does not bear the evidential

---

[10] Attorney-General's Department, *Submission 6.5*, pp. 3–4.

[11] Inspector-General of Intelligence and Security, *Submission 13*, pp.5-6.

burden in relation to these provisions.[12] The Attorney-General's Department agreed that such a provision could be included in the Bill.[13]

5.15 Alongside proposed amendments to the Bill that were provided to the Committee on 5 March 2018, the Attorney-General indicated that his 'initial view' was that the Bill should be amended by inserting a provision similar to subsection 18D(2) of the *Australian Security Intelligence Organisation Act 1979* to ensure that IGIS officials do not bear an evidential burden in relation to the defences in section 122.5 of the Bill.[14] The IGIS expressed her support, in principle, for this proposal.[15]

Partner agency officials

5.16 The Committee noted that to be lawful under the proposed secrecy provisions, foreign partners would need to rely on the statutory defence for dealing with information in accordance with an agreement with the Commonwealth (section 122.5(1)(b)) in order to share information with Australian intelligence and law enforcement agencies. The Committee asked whether framing the secrecy offences and defences in this way risked hampering co-operation with foreign partners. The Attorney-General's Department responded:

> Agencies have been consulted about the application of the offences in this context.[16]

Application to members of parliament and state and territory authorities

5.17 The Committee sought the Attorney-General's Department's advice on the extent to which members of parliament, ministers and their staff, who may deal with Commonwealth information subject to the secrecy offence, were covered by the defence in section 122.5(1). The Department initially advised that members of parliament, ministers and their staff are covered by the definition of 'Commonwealth officer', and therefore covered by the

---

12 Inspector-General of Intelligence and Security, *Submission 13*, p. 6.

13 Attorney-General's Department, *Submission 6.1*, p. 38.

14 Attorney-General, *Submission 40*, pp. 4–5.

15 Inspector-General of Intelligence and Security, *Submission 13.2*, p. 3.

16 Attorney-General's Department, *Submission 6.1*, p. 63.

defence.[17] However, after further questioning, the Department corrected this advice and confirmed that the defence at 122.5(1) would *not* be available to members of parliament who are not ministers of State.[18]

5.18 The Committee similarly sought the Department's advice on the extent to which the defence at proposed section 122.1(1) would apply to state and territory agencies—and their oversight bodies—who may be required to deal with Commonwealth information.[19] The Committee noted that while the Explanatory Memorandum makes clear that the defence at proposed section 122.1(1)(b) is intended to cover departments and agencies that 'share information with State, Territory and international counterparts, private companies, and individuals as part of their normal business dealings',[20] it was not clear that the defence would extend to state and territory oversight bodies who may be required to inspect or otherwise deal with such information in the course of their duties.

5.19 In response to both of the above concerns, the Department proposed that the issues could be addressed by amending the defence in section 122.5(1) so that it is available to any person who deals with information in their capacity as a 'public official', as defined in the existing dictionary to the *Criminal Code*, rather than to a 'Commonwealth officer', as defined in the Bill. The Department advised that the term 'public official'

- is a broader term, which explicitly covers a members of either House of Parliament,
- is used in the defences provided for in other parts of the Bill [for example, proposed section 91.4(1)], and
- extends to officers and employees of a State or Territory, individuals who hold or perform the duties of an office established by a law of a

---

17 Attorney-General's Department, *Submission 6.1*, pp. 63-64.

18 Attorney-General's Department, *Submission 6.3*, p. 1.

19 This matter was raised in *Submission 26* (name withheld), p. [3]. The submission noted that the Bill provides no exemptions for state law enforcement agencies to publish information about their own operations, capabilities, technologies, methods or sources; and that the Bill appears to provide no exemptions or defences for state law enforcement oversight authorities to deal with 'inherently harmful information' relating to the law enforcement agencies under their supervision.

20 Explanatory Memorandum, p. 276.

State or Territory and individuals who are in the service of a State or Territory (including police forces).[21]

5.20 The term 'public official' also covers the Governor-General and members of the judiciary.[22]

Oversight bodies, courts and tribunals – subsections 122.5(3)–(5)

5.21 Proposed section 122.5(3) in the Bill provides defences to the secrecy offences for communication of information to

- the IGIS and her staff,
- the Commonwealth Ombudsman and his staff, and
- the Law Enforcement Integrity Commission and staff of the Australian Commission for Law Enforcement Integrity.

5.22 The Bill also provides defences for information communicated in accordance with the *Public Interest Disclosure Act 2013* (PID Act)(proposed subsection 122.5(4)), and information communicated to a court or tribunal (proposed subsection 122.5(5)).

Limitation of defence to communication of information

5.23 Several participants in the inquiry queried why these defences were limited to only communication of information.[23] That is, they provide a defence against the secrecy offences in the Bill relating to *communication* of information, but do not provide a defence against the offences of *dealing with* information; *removing* information from or *holding* information outside a proper place of custody; or for *failing to comply with a lawful direction* regarding the retention, use or disposal of information.

5.24 For example, the Deputy Inspector-General of Intelligence and Security told the Committee that the defence in proposed subsection 122.5(3) would only apply once the communication had been completed:

---

21 Attorney-General's Department, *Submission 6.3*, p. 1.

22 *Criminal Code*, Dictionary.

23 Law Council of Australia, *Submission* 5, pp. 67, 70-71; Commonwealth Ombudsman, *Submission8*, pp. 3-4; Human Rights Law Centre, *Submission 11*, p. 19; Inspector-General of Intelligence and Security, *Submission 13*, pp. 3-4; Office of the Australian Information Commissioner, *Submission 16.1*, pp. 3-4; Joint councils for civil liberties, *Submission 31*, p. 29.

> It doesn't apply to the preparatory steps, so when a whistleblower, for want of a better word, is copying a document or scanning it to send it to us, those preparatory steps are not covered unless the person succeeds in communicating. Our comment is that we would look for protections for whistleblowers to cover all of the steps, provided they are in fact intending and acting towards communicating the information to us.[24]

5.25 The IGIS referred the Committee to existing secrecy offences in the ASIO Act and the *Intelligence Services Act 2001*, which provide specific defences for dealing with or recording information for the purpose of the IGIS exercising a power or performing a function.[25]

5.26 The Attorney-General's Department provided the following response to the concerns raised by the IGIS and other submitters:

> The defences at subsections 122.5(3), (4), (5) and (8) do not explicitly extend to conduct involving dealings with information other than communications. The defences could be explicitly extended to cover a broader range of dealings.
>
> The department notes that, in relation to security classified information, there are significant risks attached to inappropriate storage or handling of such information. An extended defence would have the effect of not criminalising improper handling of highly classified information, leaving conduct that may be preparatory to more serious offences un-addressed.[26]

5.27 Alongside proposed amendments to the Bill that were provided to the Committee on 5 March 2018, the Attorney-General indicated that his 'initial view' was that the Bill should be amended by broadening the defences at subsections 122.5(3) and (4) of the Bill to cover all dealings with information.[27] The IGIS expressed her support, in principle, for this proposal.[28]

---

24 Mr Jake Blight, Deputy Inspector-General of Intelligence and Security, *Committee Hansard*, Canberra, 31 January 2018, p. 4.

25 Inspector-General of Intelligence and Security, *Submission 13*, p. 4.

26 Attorney-General's Department, *Submission 6.1*, p. 24. See also pp. 28, 37-38, 67.

27 Attorney-General, *Submission 40*, pp. 4–5.

28 Inspector-General of Intelligence and Security, *Submission 13.2*, p. 4.

Defence for the Office of the Australian Information Commissioner

5.28 In a submission to the inquiry, the Australian Information Commissioner identified a range of functions of his office that may be impacted by the proposed secrecy offences in the Bill:

- review of *Freedom of Information Act 1982* (FOI Act) decisions of agencies and ministers
- investigate FOI Act complaints
- investigate acts or practices of entities (including Commonwealth government agencies) that may be an interference with the privacy of an individual
- receive mandatory notification from entities (including Commonwealth government agencies) about data breaches likely to cause serious harm to individuals
- conduct assessments of entities' compliance with requirements for protecting personal information under the *Privacy Act 1988* (Privacy Act)
- do all things necessary or convenient to be done for, or in connection with, the performance of the Commissioner's functions under the Privacy Act
- conduct assessments of telecommunications carriers and carriage service providers' compliance with record keeping requirements under the *Telecommunications Act 1997*.[29]

5.29 The Commissioner recommended that a defence, similar to the existing defence in proposed section 122.5(3), be included to ensure that the Office of the Australian Information Commissioner 'can continue to exercise its important oversight responsibilities'.[30]

5.30 However, the Commissioner's submission may have been based at least in part on a misreading of the Explanatory Memorandum. The Commissioner expressed concern that:

> I am unsure whether the defence proposed in section 122.5(1)—available to Commonwealth officers and others performing work for Commonwealth entities—will enable the proper exercise of my functions, duties and powers. I

[29] Office of the Australian Information Commissioner, *Submission 16.1*, p. 2.

[30] Office of the Australian Information Commissioner, *Submission 16.1*, p. 3.

> understand that the proposed defence, 'is narrow and only applies to conduct that is specifically justified or excused by a law'.[31]

5.31 The quote from the Explanatory Memorandum in the Commissioner's submission relates to the operation of existing "lawful authority" defence in section 10.5 of the Criminal Code, rather than the new defence in subsection 122.5(1) of the Bill. The full quote from the Explanatory Memorandum is:

> Section 10.5 of the Criminal Code provides a general defence of lawful authority applicable to all Commonwealth offences. This defence is narrow and only applies to conduct that is specifically justified or excused by a law. Consistent with the definition of law in the Dictionary to the Criminal Code, this means the conduct must be specifically justified or excused by a law of the Commonwealth, and includes the Criminal Code.
>
> The defence at paragraph 122.5(1)(a) is broader than the lawful authority defence available under section 10.5, and will cover a person [who] was exercising a power, or performing a function or duty, in the person's capacity as a Commonwealth officer or a person who is otherwise engaged to perform work for a Commonwealth entity, rather than the law of the Commonwealth needing to specifically justify or excuse the person's conduct.[32]

Journalists and their associates – subsection 122.5(6)–(7)

5.32 Proposed subsection 122.5(6) provides a defence for the dealing with (i.e. including communication) or holding of information that is:

a. in the public interest, and

b. in the person's capacity as a journalist engaged in fair and accurate reporting.

5.33 Proposed subsection 122.5(7) provides that dealing with or holding certain types of information is *not* in the public interest. This includes the publication of the identity of staff and affiliates of ASIO, and other intelligence agencies; information that it would be an offence to disclose under certain sections of the *Witness Protection Act 1994*; and information that 'will or is likely to harm or prejudice the health or safety of the public or a section of the public'.

---

31 Office of the Australian Information Commissioner, *Submission 16.1*, p. 3.

32 Explanatory Memorandum, pp. 275–276.

5.34 Many participants in the inquiry raised concerns about the impact of the secrecy provisions on journalists, including the limited coverage of these defences.[33] A submission from the joint media organisations—representing 14 major media organisations, including News Corp Australia, Fairfax media, the Australian Broadcasting Corporation, FreeTV Australia, Commercial Radio Australia and the Media, Entertainment and Arts Alliance—asserted that the Bill

> criminalises all steps of news reporting, from gathering and researching of information to publication/communication, and applies criminal risk to journalists, other editorial staff and support staff that knows of the information that is now an offence to 'deal' with, hold and communicate.
>
> The Bill is a significant step beyond the existing legislation that applies to Commonwealth officers. This is particularly when it has not been demonstrated that there are 'problems' that need to be 'fixed'. The result is that fair scrutiny and public interest reporting is increasingly difficult and there is a real risk that journalists could go to jail for doing their jobs.[34]

5.35 Many of the concerns raised by the media organisations relate to the breadth of information and conduct captured by the secrecy offences, including their application to both 'insiders' and 'outsiders', as was discussed in the previous chapter. The organisations recommended a 'general public interest/news reporting defence' in the Bill and described the existing defence for journalists in proposed subsection 122.5(6) as being 'narrow and subjective, particularly the matters of "public interest" and "fair and accurate reporting"'. In relation to the existing defence, the organisations recommended:

---

33 E. Anne Lanham, *Submission 3*; Lucy Strang, *Submission 4*; Law Council of Australia, *Submission 5*, p. 67; Australian Lawyers for Human Rights, *Submission 7*, p. 6; Joint media organisations, *Submission 9*; Human Rights Watch, *Submission 10*, p. 1; Human Rights Law Centre, *Submission 11*, p. 19; Australian Lawyers Alliance, *Submission 12*, p. 16; Valerie Heath, *Submission 14*, p. 2; Dr Lawrence McNamara, University of York, *Submission 19*, p. 3; Centre for Media Transition, University of Technology, Sydney, *Submission 23*, pp. 3, 6–7; Chris Morris, *Submission 25*; United Nations Special Rapporteurs, *Submission 30*, p. 8; Joint councils for civil liberties, *Submission 31*, pp. 31–35; Digital Rights Watch, *Submission 34*, p. [3].

34 Joint media organisations, *Submission 9*, p. 1.

- that ambiguity as to whether the defence applies to communications offences, as well as 'deals with' offences, be removed,[35]
- that 'journalist' be defined in the Bill consistently with the definition in the *Evidence Act 1995*,
- that the defence be extended to journalist's support staff, who may also deal with the information covered by the offences,
- that the use of the term 'fair and accurate reporting' be reconsidered,
- that the Committee review the Journalists Information Warrant Scheme, noting concerns that powers under the *Telecommunications (Interception and Access) Act* could be used to identify a journalist's confidential source, and
- that the inclusion of 'harm or prejudice the health or safety of the public or a section of the public' be removed from proposed subsection 122.5(7).[36]

5.36 These points were raised in similar terms and supported by some other contributors to the inquiry.

5.37 The Centre for Media Transition additionally argued that the defence should be 'recast' as an exemption from the offence provisions, or 'at least that the burden of proof be on the prosecution to establish that a journalist was not working in the public interest'.[37]

5.38 The Law Council of Australia recommended that the Bill

> non-exhaustively identify some factors that may be considered for the purposes of determining whether the dealing with or holding of information may be in the public interest for the purpose of the proposed journalist defence. Such factors may include for example:
>
> - promoting open discussion of public affairs, enhancing government accountability or contributing to positive and informed debate on issues of public importance;

---

35 While the term 'deals' is defined in the Bill to include communication, it was separately submitted that the explicit separation of offences for 'communication' and 'deals with' offences in proposed sections 122.1 and 122.1, and a lack of clarify in the Explanatory Memorandum, may cast doubt over the scope of the protection. See Centre for Media Transition, University of Technology, Sydney, *Submission 23*, p. 5.

36 Joint media organisations, *Submission 9*, pp. 4–8.

37 Centre for Media Transition, University of Technology, Sydney, *Submission 23*, p. 5.

- informing the public about the policies and practices of agencies in dealing with members of the public;
- ensuring effective oversight of the expenditure of public funds;
- the information is personal information of the person to whom it is to be disclosed; and
- revealing or substantiating that an agency (or a member of an agency) has engaged in misconduct or negligent, improper or unlawful conduct.[38]

5.39 Responding to the Law Council's suggestion, the Attorney-General's Department advised:

> The Bill does not seek to define public interest beyond the exclusions listed in subsection 122.5(7). This allows the defendant to adduce or point to evidence that suggests a reasonable possibility that the person held or dealt with the information in the public interest (as required in order to discharge an evidential burden consistent with subsection 13.3(6) of the Criminal Code). Once this burden is discharged, the prosecution will then be required to prove the person did not hold or deal with the information in the public interest beyond reasonable doubt.[39]

Government proposed amendments – journalists defence

5.40 On 13 February 2018, the Attorney-General's Department advised the Committee that it had been asked by the Attorney-General to progress a number of changes to the general secrecy offences in Schedule 2 to the Bill. This included amendments directed at 'strengthening the defence for journalists' at proposed subsection 122.5(6) by

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

---

38 Law Council of Australia, *Submission 5*, p. 70.

39 Attorney-General's Department, *Submission 6.1*, p. 22.

5.41 The Committee received draft amendments to this effect from the Attorney-General on 5 March 2018.[40] The proposed amendments remove the existing defence at subsection 122.5(6), and replace it with the following defence:

> It is a defence to a prosecution for an offence by a person against this Division relating to the dealing with or holding of information that:
>
> (a) the person dealt with or held the information in the person's capacity as a person engaged in reporting news, presenting current affairs or expressing editorial content in news media; and
>
> (b) at that time, the person reasonably believed that dealing with or holding the information was in the public interest (see subsection (7)).[41]

5.42 Additionally, subsection 122.5(7) is proposed to be amended to provide that a person may not reasonably believe that dealing with or holding information is in the public interest if—in relation to non-Commonwealth officers only—dealing with or holding information that, at that time, 'will or is likely to result in the death of, or serious harm to, a person'. This differs from the existing criteria, which will continue to apply in relation to Commonwealth officers, that the conduct 'will or is likely to harm or prejudice the health or safety of the Australian public or a section of the Australian public'.

5.43 Subsection 122.5(7) is also proposed to be amended to provide that a person may not reasonably believe that dealing with or holding information is in the public interest if the dealing with or holding of the information is 'for the purpose of directly or indirectly assisting a foreign intelligence agency or a foreign military organisation'.[42]

5.44 Responding to the proposed amendments, submitters expressed general support for the amendments but noted remaining concerns about the

---

40 Attorney-General, *Submission 40 and 40.1*.

41 Attorney-General, *Submission 40.1*, p. 5 (amendment No. 36).

42 Under the proposed amendments, a new definition of 'foreign military organisation' is proposed to be added to section 121.1 of the *Criminal Code*. 'Foreign intelligence agency' is already proposed to be defined in the Dictionary to the *Criminal Code* under item 24 of the Bill.

applicability of the defence to non-traditional forms of journalism; and the perceived lack of protection for persons who are not journalists.[43]

5.45 The Law Council of Australia submitted that it

> remains opposed to the notion that the public interest exception should only be available to journalists or the news media. This is not a proper criterion for criminal liability. The exception is now defined more widely than journalism but just who the target is remains unclear. The defence refers to news media but it is not clear that it would pick up an individual blogging for example.[44]

5.46 The Law Council noted that the amended defence 'still reaches only people who are engaged in the news media' and would not protect 'a victim of prosecutional police malpractice, for example'.[45]

5.47 The joint media organisations expressed concern that the amended defence would not specifically extend to editorial support staff, such as legal advisors and administrative staff; and that it would apply to a 'narrow range of news media formats'. The organisations recommended that paragraph 122.5(6)(a) be amended to read:

> *The person dealt with or held the information in the person's capacity as a person engaged <u>in the business of</u> reporting news, presenting current affairs or expressing editorial <u>or other</u> content in news media.*[46] [emphasis in original]

5.48 The joint media organisations also considered that support staff should 'not be required to hold the belief that dealing with the information was in the public interest in order to rely on the defence',[47] as assessing whether or not something is in the public interest is 'not within their capacity in the normal course of their job'.[48] The organisations recommended the Bill being amended in one of two ways:

---

43 Law Council of Australia, *Submission 5.1*, pp.2, 5; Australian Lawyers for Human Rights, *Submission 7.1*, p. 2; Joint media organisations, *Submission 9.2*, p. 4; Human Rights Law Centre, *Submission 11.2*, p. 4; Joint councils for civil liberties, *Submission 31.1*, p. 5.

44 Law Council of Australia, *Submission 5.1*, p. 5.

45 Dr David Neal SC, Member, National Criminal Law Committee, Law Council of Australia, *Committee Hansard*, Melbourne, 16 March 2018, p. 8.

46 Joint media organisations, *Submission 9.2*, pp. 4–5.

47 Joint media organisations, *Submission 9.2*, p. 5.

48 Ms Georgia-Kate Schubert, Head of Policy and Government Affairs, News Corp Australia, *Committee Hansard*, Melbourne, 16 March 2018, p. 25.

Amend s122.5(6)(b) so that it contains two sub-sections:

(b) at that time, the person:

(i) reasonably believed that dealing with the information was in the public interest (see subsection (7)); or

(ii) was acting at the direction or under the instructions of a person who held such a belief

OR

Amend s122.5(6)(b) so that it only relates to a person undertaking an activity which falls within subsections (f), (g), (i) and (j) of the definition of 'deals' with activity (h) 'communicates' excluded by operation of section 122.4A(2)(a).[49]

5.49 Finally, the joint media organisations recommended framing proposed section 122.5(6) as an exemption for public interest reporting, rather than as a defence.[50] The organisations submitted:

> While the evidentiary burden may be the same for a defence and an exemption we continue to hold that to minimise the chilling effect on public interest reporting it would be significantly better to have an exemption rather than a defence.[51]

5.50 Responding to the joint media organisations' supplementary submission, the Attorney-General's Department stated its view that 'some of the amendments proposed in that submission are not necessary', and that the amended Bill 'strikes an appropriate balance'.[52] The Department noted, however, that it was 'open to suggestions' as to how the defence

> could be broadened to cover the types of staff who are legitimately involved in the reporting of news media but not so broad that it can cover everyone

---

49 Joint media organisations, *Submission 9.2*, p. 5.

50 Joint media organisations, *Submission 9.2*, p. 5; Mr Paul Murphy, Chief Executive, Media Entertainment and Arts Alliance, *Committee Hansard*, Melbourne, 16 March 2018, pp. 25–26.

51 Joint media organisations, *Submission 9.2*, p. 3.

52 Ms Anna Harmer, First Assistant Secretary, Attorney-General's Department, *Committee Hansard*, Melbourne, 16 March 2018, p. 36.

regardless of whether they are actually connected to that process of reporting the news.[53]

5.51 The Department disagreed with the joint media organisations' suggestion that an exemption would arise at a different point of the process than a defence.[54] The Department stated that 'an exception operates in precisely the same way as a defence', and that defences are considered by both the Australian Federal Police and the Director of Public Prosecutions in determining whether to prosecute or investigate and offence.[55]

5.52 The Director-General of Security cautioned against any proposal to exempt journalists from the provisions, noting that 'if that particular class is exempt from the legislation it will automatically become a target for foreign intelligence services'.[56] ASIO considered that such an exclusion would 'fundamentally undermine the effectiveness of the legislation'.[57]

External whistleblowers

5.53 In addition to journalists, many participants in the inquiry considered that the secrecy offences in the Bill should not apply to journalists' sources and other whistleblowers who disclose information outside internal government mechanisms, such as the *Public Interest Disclosures Act 2013* (PID Act).[58]

---

53 Ms Tara Inverarity, Assistant Secretary, Attorney-General's Department, *Committee Hansard*, Melbourne, 16 March 2018, p. 39.

54 See Ms Georgia-Kate Schubert, Head of Policy and Government Affairs, News Corp Australia, *Committee Hansard*, Melbourne, 16 March 2018, p. 26.

55 Ms Anna Harmer, First Assistant Secretary, Attorney-General's Department, *Committee Hansard*, Melbourne, 16 March 2018, p. 36.

56 Mr Duncan Lewis, Director-General of Security, Australian Security Intelligence Organisation, *Committee Hansard*, Melbourne, 16 March 2018, p. 37.

57 Mr Duncan Lewis, Director-General of Security, Australian Security Intelligence Organisation, *Committee Hansard*, Melbourne, 16 March 2018, p. 35.

58 Benji Wakely, *Submission 1*; E. Anne Lanham, *Submission 3*; Lucy Strange, *Submission 4*; Law Council of Australia, *Submission 5*, p. 67; Australian Lawyers for Human Rights, *Submission 6*, p. 6; Human Rights Watch, *Submission 10*, p. 7; Human Rights Law Centre, *Submission 11*, pp. 7–8, 17–18; Australian Lawyers Alliance, *Submission 12*, pp. 15–16, 17; Australian Human Rights Commission, *Submission 17*, p. 5; Dr Lawrence McNamara, University of York, *Submission 19*, p. 3; Centre for Media Transition, University of Technology, Sydney, *Submission 23*, p. 6; United Nations Special Rapporteurs, *Submission 30*, p. 8; Joint councils for civil liberties, *Submission 31*, pp. 33–34; Digital Rights Watch, *Submission 34*; WWF-Australia, *Submission 36*, p. 2; Get Up!, *Submission 38*, p. 3.

5.54 In its submission, the Attorney-General's Department summarised the range of internal mechanisms available to whistleblowers who are Commonwealth officers:

> 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.[59]

5.55 The Human Rights Law Centre regarded the internal disclosure mechanisms, such as the PID Act, as providing inadequate protection for the purpose of the general secrecy offences in the Bill:

> The first element of a proportionate approach is the existence of robust processes for lawful public interest disclosure by government employees and others who are in possession of government information. The best way to ensure a balance between government accountability and protecting information, the release of which would cause serious harm to a public interest, is to provide a sufficiently independent lawful release valve for information in the public interest, immune from sanctions. This reduces the need for a whistleblower to engage in unauthorised sharing of information to, for instance, expose malfeasance or dishonest information provided to the public by a politician. A complement to the internal avenue for public interest disclosure is the ultimate power of a court to determine, in the event of external disclosure, whether the disclosure, on balance, was in the public interest. This safeguard, which may be very rarely engaged, is necessary in the event that internal processes are ineffective, delayed or compromised. It is especially vital where a person is facing criminal conviction, rather than, say disciplinary action or the loss of employment.[60]

5.56 The Centre considered that the 'sheer breadth' of the Bill's secrecy offences created 'significant risks' that the defences in proposed section 122.5 would

---

59 Attorney-General's Department, *Submission 6*, p. 33.

60 Human Rights Law Centre, *Submission 11*, pp. 7–8.

'not sufficiently protect the public interest'. It noted several 'gaps' between the protection available in the PID Act and the provisions of the Bill. These gaps included that while the secrecy offences in the Bill apply to any person, the PID Act is only available to public officials (as defined in the Act). The Centre suggested that the most 'obvious and logical' way to address this gap was to limit the offences to the same set of public officials that are covered by the PID Act, with more limited subsequent disclosure offences applicable to other persons.[61]

5.57 Several participants in the inquiry—including the Law Council of Australia and the Human Rights Law Centre—called for there to be a general 'public interest' defence available to protect disclosures that are made outside the Commonwealth government's internal whistleblowing mechanisms.[62]

5.58 The Law Council pointed out that the defences in proposed section 122.5 would not capture disclosures made under private sector whistleblower laws, for example under the *Corporations Act 2001*.[63]

5.59 The Committee sought further information from the Attorney-General's Department in response to the concerns raised by submitters about the lack of protection for external whistleblowers. The Department advised:

> There are established mechanisms for Commonwealth officers to make public interest disclosures under the Public Interest Disclosure Act. The inclusion of a general public interest defence would disrupt the primacy of the Public Interest Disclosure Scheme as the mechanism for making disclosures of information.
>
> The defence in subsection 122.5(4) could be broadened to cover other Commonwealth public interest disclosure schemes. The department notes however that neither it nor submissions have identified circumstances in which whistleblowers under other schemes would be dealing with inherently harmful information or information that causes harm to Australia's interests.[64]

---

61 Human Rights Law Centre, *Submission 11*, p. 18.

62 Benji Wakely, *Submission 1*; Law Council of Australia, *Submission 5*, pp. 67–70; Joint media organisations, *Submission 9*, pp. 1, 8; Australian Lawyers Alliance, *Submission 12*, p.17; Australian Human Rights Commission, *Submission 17*, p. 5; Joint councils for civil liberties, *Submission 31*, pp. 33–35; *Submission 31.1*, p. 10; GetUp, *Submission 38*, p. 3.

63 Law Council of Australia, *Submission 5*, pp. 67, 70.

64 Attorney-General's Department, *Submission 6.1*, p. 66. See also pp. 22, 36, 42.

5.60 At a subsequent public hearing, the Law Council of Australia identified that reporting the misuse of power in a police investigation—which could be said to be 'interfering' with the investigation—is an example of conduct that could be captured by the provisions of proposed section 122.2, but for which there would not currently a public interest defence available in the Bill.[65]

5.61 In response, the Department acknowledged that the PID Act would not cover this type of whistleblowing, but stated that

> it doesn't mean that there aren't means to bring that malpractice, corruption or whatever is alleged to the appropriate authorities without publication of it in the media.[66]

Information that has been previously communicated or made public – subsections 122.5(2) and (8)

5.62 The Attorney-General's Department noted that the 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'.[67] It highlighted the two defences available in the Bill's secrecy provisions in relation to information that has previously been communicated or made public:

- proposed subsection 122.5(2), in relation to all of the secrecy offences, where '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', and
- proposed subsection 122.5(8), in relation to the secrecy offences concerning communication of information, where
  - a person did not make or obtain the information by reason of his or her being a Commonwealth officer, being otherwise engaged to perform work for a Commonwealth entity, or under an arrangement or agreement with the Commonwealth, and
  - the information has already been communicated, or made available, to the public (the 'prior publication'), and

---

65 Dr David Neal SC, Member, National Criminal Law Committee, Law Council of Australia, *Committee Hansard*, Melbourne, 16 March 2018, p. 8.

66 Ms Tara Inverarity, Assistant Secretary, Attorney-General's Department, *Committee Hansard*, Melbourne, 16 March 2018, p. 40.

67 Attorney-General's Department, *Submission 6*, p. 33.

- the person was not involved in the prior publication, and
- at the time of the communication, the person believes that the communication will not cause harm to Australia's interests or the security or defence of Australia, and
- having regard to the nature, extent and place of the prior publication, the person has reasonable grounds for that belief.

5.63 The defence at subsection 122.5(2) is intended to apply to information communicated 'to the public at large, to a segment of the public, or to individual members of the public or a segment of the public on request', 'even if no member of the public actually obtains or collects the information'.[68] This includes, for example,

- information included in a speech or interview given in public or to a professional forum,
- information posted on a publicly-accessible website, even if no one visits the website, and
- information members of the public are entitled to request access to, even if no members of the category do request access to it.[69]

5.64 The defence at subsection 122.5(8) is drafted in similar terms to the prior publication defence contained in subsection 35P(3A) of the ASIO Act, which was inserted following a recommendation of the then- Independent National Security Legislation Monitor, the Hon Roger Gyles AO QC.[70] An example of where the defence would apply includes where a person communicates information about law enforcement operation conducted in public.[71] The Explanatory Memorandum provides the following example where further publication of information already in the public domain could cause harm:

> [W]here information is brought into the public domain inadvertently, such as where a security classified document or information provided to the Australian Government in accordance with a legal obligation is revealed as a result of a technical or administrative error. Where steps are quickly taken to reverse the disclosure, subsequent publication of that information is likely to

68 Explanatory Memorandum, p. 277.

69 Explanatory Memorandum, p. 277.

70 Explanatory Memorandum, p. 283.

71 Explanatory Memorandum, pp. 230, 231.

> bring that information to the attention of a much greater number of people and could result in considerable new or additional harm.[72]

5.65 Several participants in the inquiry raised concerns about the about the defence at proposed subsection 122.5(2) being limited to information made public 'with the authority of the Commonwealth'.[73] For example, Australian Lawyers for Human Rights submitted that it was 'not clear how a defendant will know whether or not this is the case'.[74] The joint media organisations argued that 'it should be a defence that the information has already been communicated or made available to the public—regardless of the status of the Commonwealth's authorisation of that information'.[75] One submission noted that, due to the limitations in both of the prior publication defences, it would be an offence, carrying a penalty of up to 10 years imprisonment, to buy a copy of a newspaper containing an article containing 'inherently harmful information'.[76]

5.66 The Australian Human Rights Commission agreed that limiting the defence to information made public 'with the authority of the Commonwealth' was 'not really in accord with' principle 17 of the Johannesburg Principles on National Security, Freedom of Expression and Access to Information. The Johannesburg Principles state:

> Once information has been made generally available, by whatever means, whether or not lawful, any justification for trying to stop further publication will be overridden by the public's right to know.[77]

---

72 Explanatory Memorandum, p. 283.

73 Australian Lawyers for Human Rights, *Submission 7*, p. 6; *Submission 7.1*, p. 2; Joint media organisations, *Submission 9*, p. 4; Australian Human Rights Commission, *Submission 17*, pp. 4–5; *Submission 26* (name withheld), p. [2]; Joint councils for civil liberties, *Submission 31*, pp. 29–30;

74 Australian Lawyers for Human Rights, *Submission 7*, p. 6.

75 Joint media organisations, *Submission 9*, p. 4.

76 *Submission 26* (name withheld), p. [2]. The submission noted that while proposed section 122.5(8) provides a defence relating to the communication of information which is already available to the public, it does not apply to offences relating to dealing with information.

77 Mr John Howell, Senior lawyer, Australian Human Rights Commission, *Committee Hansard*, Canberra, 31 January 2018, p. 50. See also Australian Human Rights Commission, *Submission 17*, p. 9. It is noted that Australian Government is not a signatory to the Johannesburg Principles.

5.67 The Commission noted that communication of information that has already been made public through unauthorised disclosure will 'not necessarily further harm the interests of the Commonwealth'. It recommended that the defence provisions 'be drafted to ensure they apply to (at least) disclosures of information that is already widely known or easily accessible'.[78]

5.68 In relation to the defence at proposed subsection 122.5(8), the Australian Lawyers Alliance submitted that the requirement for a person to believe, on reasonable grounds, that their communication will not cause harm to Australia's interests or the security or defence of Australia 'is an extraordinarily high bar for a defendant to reach in seeking to defend their actions'. The Alliance expressed the view that it should be up to the prosecution to show that the defendant had intended to cause harm.[79]

5.69 The joint media organisations submitted that the requirements of paragraphs 122.5(8)(d) and (e) would 'intimidate news organisations from being the first to publish' and lead to 'a substantial chilling of public interest journalism'.[80]

5.70 The Attorney-General's Department explained why the requirements of paragraphs (d) and (e) were necessary as follows:

> Just because information has previously been published anywhere does not mean that further publication of that information can't cause significant harm. The obvious example is a document leaked that discloses the identities of Australian intelligence officers around the world. In fact, subsequent publication will amplify the harm that can come from that disclosure by making it more broadly available and therefore leading to much graver risks of harm to those individuals.[81]

5.71 Similar to above discussion relating to oversight bodies, concerns were also raised that the defence at proposed section 122.5(8) is limited to *communication* of information, and does not cover other dealings.[82] The

---

78 Australian Human Rights Commission, *Submission 17*, pp. 4–5.

79 Australian Lawyers Alliance, *Submission 12*, p. 17.

80 Joint media organisations, *Submission 9*, p. 7.

81 Ms Tara Inverarity, Assistant Secretary, Attorney-General's Department, *Committee Hansard*, Melbourne, 16 March 2018, p. 39.

82 Law Council of Australia, *Submission 5*, pp. 69-71; Australian Human Rights Commission, *Submission 17*, p. 5.

Committee noted that there appeared to be no defence available for a member of the public who downloads a copy of a leaked document from a whistleblowing website in order to view it (i.e. the person has 'dealt with' the information); but that a defence would become available if that same person also emailed a copy of the document to some friends (i.e. the person has communicated the information). The Department advised that the defence at section 122.5(8) 'could be explicitly extended to cover a broader range of dealings', but noted the 'significant risks attached to inappropriate storage or handling of such information'.[83]

Information relating to a person – subsection 122.5(9)

5.72 Proposed subsection 122.5(9) provides a defence against the secrecy offences in relation to dealing with (i.e. including communicating) information if:

- a person did not make or obtain the information by reason of his or her being a Commonwealth officer, being otherwise engaged to perform work for a Commonwealth entity, or under an arrangement or agreement with the Commonwealth, and
- the person believes that their making or obtaining of the information was required or authorised by law, and
- having regard to the circumstances of the making or obtaining of the information, the person has reasonable grounds for that belief, and
- the person communicates the information to the person to whom it relates; the person is the person to whom the information relates; or the dealing is in accordance with the express or implied consent of the person to whom the information relates.

5.73 The Law Council of Australia recommended that this defence be reconsidered. The Law Council referred to the ALRC's consideration that this kind of disclosure was

> not appropriate in all circumstances, noting that it may be sensitive for other reasons—for example, it may be personal information about one individual that is relevant to an ongoing investigation into the criminal activities of another individual.[84]

5.74 The Attorney-General's Department responded that it

---

83 Attorney-General's Department, *Submission 6.1*, pp. 24, 67.

84 Law Council of Australia, *Submission 5*, p. 69, citing Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, Report 112, December 2009, pp. 248–249.

> believes this defence is necessary and prevents the criminal offences from operating too broadly, in situations where a person has consented to their information being dealt with, even if it is inherently harmful information.[85]

5.75 The Department referred to the following examples in the Explanatory Memorandum in which it was intended that the defence would 'ensure that a person is not inappropriately subject to criminal liability':

- Example 1: Person A give[s] taxation information to the Australian Taxation Office as part of their income tax return, as required by section 161 of the *Income Tax Assessment Act 1936*. Person A then communicates the same information to their bank, as part of an application for a mortgage.
- Example 2: Person B is the accountant for Person C. Person B has lodged Person C's income tax return on Person C's behalf. Person B gives Person C a copy of the tax return as lodged.
- Example 3: Person D has received a notice issued under an Act requiring them to provide a Commonwealth agency with information that relates to Person D. Person D gives the agency the information specified in the notice. The Act does not contain a specific secrecy provision limiting the disclosure of information about the notice. Person D subsequently shows Person E the notice and the information that Person D gave to the agency in accordance with the notice.[86]

Legal advice

5.76 The submission from Ms Valerie Heath also noted the current lack of a defence providing for the disclosure to or receipt by a lawyer of information 'for the purpose of the person receiving legal advice about how to make a protected disclosure'.[87]

5.77 The Law Council of Australia recommended that an exception be included in the Bill where conduct is engaged in for the purpose of obtaining legal advice in relation to a matter the subject of an offence. The Law Council submitted:

> This is particularly important given the definition of 'causing harm to Australia's interests' in proposed paragraph 121.1(c) includes 'harm or

---

85 Attorney-General's Department, *Submission 6.1*, p. 23.

86 Explanatory Memorandum, p. 284.

87 Valerie Heath, *Submission 14* , p. 2.

> prejudice Australia's international relations in relation to information that was communicated in confidence'. This would potentially capture a lawyer engaged to represent a government, authority or organisation, who communicates or receives information on behalf of their client.[88]

5.78 The Department responded:

> It is not the intention to cover situations where a person is seeking legal advice about their ability to make a public interest disclosure or in relation to the application of the defences.[89]

5.79 The Committee asked the Department whether the defence in proposed subsection 122.5(9) (as discussed above) was intended to allow a person to deal with information for the purpose of seeking legal advice. The Department responded:

> It is not the intention of the offences to cover situations where a person is seeking legal advice about their ability to communicate information, or the application of the offences. A specific defence could provide clarity in relation to such activities.[90]

5.80 The Law Council also recommended that the provisions include an exception, similar to the exception in paragraph 35P(3)(b) of the ASIO Act, providing that the offence provisions 'do not apply if the disclosure was for the purposes of any legal proceedings arising out of or otherwise related to the Division or of any report of any such proceedings'.[91]

5.81 The Department responded as follows:

> The existing defence at subsection 122.5(5) relating to provision of documents to a court or tribunal ensures that the offence does not criminalise making disclosures of information for the purposes of legal proceedings.[92]

Committee comment

5.82 As noted earlier, the broad range of conduct captured by the Bill's secrecy offences means that it is essential that a robust set of defences (or exceptions)

---

88 Law Council of Australia, *Submission 5*, p. 69.

89 Attorney-General's Department, *Submission 6.1*, p. 22.

90 Attorney-General's Department, *Submission 6.1*, p. 68.

91 Law Council of Australia, *Submission 5*, p. 69.

92 Attorney-General's Department, *Submission 6.1*, p. 23.

is available for innocuous conduct. While the Bill currently contains a range of defences that cover many of these circumstances, evidence during the inquiry suggested that further amendments are required to address gaps in the available defences and ensure the offences are appropriate targeted. In making recommendations, the Committee is mindful to ensure that the provisions remain effective in deterring unauthorised dealings with sensitive information.

Official duties

5.83 Proposed subsection 122.5(1) provides a defence for persons exercising powers, or performing functions or duties, as Commonwealth officers (or persons otherwise engaged to perform work for a Commonwealth entity). The subsection also provides a defence for conduct in accordance with an arrangement or agreement with the Commonwealth that allows for the exchange of information.

5.84 The Committee notes the particular difficulty that the IGIS and her staff could face in meeting the evidential burden for the defence in 122.5(1) due to their specific legislative obligation not to disclose information obtained in the course of their duties to any person, or to a court. The Committee recommends that the Bill be amended to take these circumstances into account.

Recommendation 25

5.85 The Committee recommends that the Bill be amended to ensure that staff of the Inspector-General of Intelligence and Security are appropriately protected, noting the limitations on the Inspector-General and members of staff of the Inspector-General giving evidence under the *Inspector-General of Intelligence and Security Act 1986*. The Committee recommends that this amendment be developed in consultation with the Inspector-General and her Office.

Defences limited to communication of information

5.86 Several participants in the inquiry pointed out that while the Bill includes offences that cover both communications and broader 'dealings' with certain information, several of the defences in Bill only extend to communications. While noting that there are risks associated with broadening the defence to all dealings, the Committee considers it would be unacceptable for there to

be a defence available for a person to communicate information to certain entities, but no defence available for that person to deal with that information as they prepare to communicate it.

Recommendation 26

5.87 The Committee recommends that the following proposed defences be broadened to cover all dealings with information, rather than being limited to communication of information:

- **proposed section 122.5(3) – relating to the Inspector-General of Intelligence and Security, the Commonwealth Ombudsman and the Law Enforcement Integrity Commissioner,**
- **proposed section 122.5(4) – relating to the *Public Interest Disclosure Act 2013*,**
- **proposed section 122.5(5) – relating information provided to a court or tribunal, and**
- **proposed section 122.5(8) – relating to information that has been previously communicated.**

Public interest defence for journalists

5.88 The Committee notes the views of a range of participants in the inquiry that the defence at proposed subsection 122.5(6) of the Bill is too narrow and subjective. The Committee therefore welcomes the Attorney-General's proposed amendments to the Bill which remove the requirement for journalists to demonstrate that their reporting was 'fair and accurate' and extends the defence to a broader range of staff.

5.89 The Committee notes that the joint media organisations have expressed a small number of remaining concerns about the drafting of the defence, and considers that that further refinement may be required. This includes refinements in relation to the breadth of news media formats covered by the defence; the extent to which editorial support staff are included; and the requirement for support staff to hold a belief in relation to the public interest. The Committee recommends that the Government consider further amendments to the proposed defence in order to address these concerns.

Recommendation 27

5.90 The Committee recommends that the Attorney-General's proposed amendments to the defence for journalists at proposed section 122.5(6), and the associated amendments at 122.5(7), be implemented. This includes expanding the defence to all persons engaged in reporting news, presenting current affairs or expressing editorial content in news media where the person reasonably believed that dealing with or holding the information was in the public interest.

The Committee also recommends that the Government consider further refinements to the proposed defence in order to

- **make explicit that editorial support staff are covered by the defence, including legal advisors and administrative staff,**
- **ensure editorial staff and lawyers, who are engaging with the substance of the information, be required to hold a reasonable belief that their conduct is in the public interest, and**
- **allow administrative support staff working at the direction of a journalist, editor or lawyer who holds the reasonable belief, to benefit from the defence.**

5.91 The Committee notes the Attorney-General's and his Department's advice that reframing the defence as an exception would make no practical difference. In either case, the evidential burden would be on the defendant to adduce or point to evidence that suggests a reasonable possibility that the defence or exception applies, after which the prosecution would need to disprove the defence or exception beyond reasonable doubt.[93]

5.92 The Committee also considers that it would not be appropriate to recast the defence as an element of the offence. As journalists are not public officials, and would only deal with information subject to the offence at proposed section 122.4A on an exceptional basis, it would burdensome and costly for a

93 See Attorney-General's Department, *Submission 6.5*, pp. 1–2.

prosecution to be required to prove in *all* cases that the defendant is *not* a journalist engaged in public interest reporting.[94]

5.93 Moreover, the Committee does not support any proposal to entirely exempt journalists from the provisions. The Committee particularly notes the Director-General of Security's concerns that such an exemption would make journalists a target for foreign intelligence services and 'fundamentally undermine the effectiveness of the legislation'.[95]

5.94 The Committee notes that the effect of proposed subsection 122.5(7) is to place limits on the conduct that may be reasonably believed to be in the public interest for the purpose of the defence for journalists at subsection 122.5(6). However, the inclusion of both subparagraphs of paragraph 122.5(7)(d) gives rise to technical difficulties in the Bill, primarily due to use of similar language in the elements of the offence (see the Attorney-General's proposed section 122.4A(1)(d)(iv)). Noting these difficulties, and given that the defendant would already need to convince the court that dealing with or holding of information was in the public interest, the Committee does not consider either limitation on the availability of the defence to be necessary.

Recommendation 28

5.95 The Committee recommends that the Bill be amended to remove proposed paragraph 122.5(7)(d), which currently limits the availability of the defence for persons engaged in reporting news.

Defences for whistleblowers

5.96 The Committee acknowledges the concerns of a number of participants in the inquiry that while a public interest defence is available to journalists, there is not an equivalent defence available to other persons acting in the public interest.

5.97 The Committee notes that the *Public Interest Disclosure Act 2013* (PID Act) provides clear processes for Commonwealth officers to report wrongdoing and maladministration in the public sector. Communications under the PID Act are appropriately covered by the defence at proposed subsection

---

94 See Attorney-General's Department, *Submission 6.5*, pp. 2–4.

95 Mr Duncan Lewis, Director-General of Security, Australian Security Intelligence Organisation, *Committee Hansard*, Melbourne, 16 March 2018, p. 35.

122.5(4). The Committee supports the primacy of the PID Act as the mechanism for Commonwealth officers to disclose information concerning wrongdoing and maladministration, and considers that introducing a broader public interest defence that extended to Commonwealth officers would undermine this role.

5.98 While there is not an all-encompassing public interest defence in the Bill for non-Commonwealth officers, there are a range of defences available to those who have a legitimate need to deal with information captured under the proposed secrecy offences.[96]

5.99 Of these defences, the Committee notes that the defence for information that has already been communicated at proposed subsection 122.5(8) appears to be intended to provide the broadest protection for non-Commonwealth officers.[97] As the defence applies to information that has 'already been communicated, or made available to the public', it would protect a person who is not a journalist from being guilty of a secrecy offence as long as they

- were not involved in the prior publication/communication, and
- believed, on reasonable grounds, that their communication of (or other dealing with, if the above recommendation is accepted) the information will not 'cause harm to Australia's interests'.[98]

5.100 For example, the defence could protect a member of the public who downloaded, copied or shared 'inherently harmful information' that had been previously published on the internet as a result of an unauthorised disclosure, so long as the person believed their conduct would cause no

---

96 Specific defences available to non-Commonwealth officers include the defence in relation to information that is already public (with the authority of the Commonwealth) at proposed subsection 122.5(2), the defence in relation to information communicated to the IGIS, the Commonwealth Ombudsman and the Australian Commission for Law Enforcement Integrity at proposed subsection 122.5(3), the defence in relation to information communicated to a court or tribunal at proposed subsection 122.5(4), the defence for journalists at proposed subsection 122.5(6), and the defence for information that has already been communicated at proposed subsection 122.5(8).

97 Subject to the defence being extended to cover other dealing with information, as well as communication of information, as recommended above.

98 Subsection 122.5(8) currently also provides that the person believes that the communication will not cause harm to the 'security or defence of Australia'; however, this would no longer be necessary if security and defence is moved into the definition of 'cause harm to Australia's interests, as recommended above.

further harm. Similarly, a member of the public who received and passed on classified information that had been misplaced due to an administrative error, such as in the recent high-profile example of the 'Cabinet Files',[99] would have a defence if the person believed their handling of the documents did not 'cause harm to Australia's interests'.

5.101 Accordingly, the Committee does not consider that an additional, more broadly drafted public interest defence is necessary in the Bill.

5.102 However, the Committee notes that, as discussed above, the definition of 'cause harm to Australia's interests' includes to interfere with or prejudice the prevention, detection, investigation, prosecution and punishment of Commonwealth criminal offences, and other AFP functions under the *Australian Federal Police Act 1979* and the *Proceeds of Crimes Act 2002*. As a result, proposed subsection 122.5(8) may not protect a person who wished to report misconduct or maladministration in, for example, the investigation of a Commonwealth criminal offence, as it would be difficult for that person to claim that their reporting of the wrongdoing did not interfere with the investigation.

5.103 While the defence at proposed subsection 122.5(3) would cover reporting to the Australian Commission for Law Enforcement Integrity, the Committee considers a stronger defence is necessary to cover the full range of organisations that may be involved in the prevention, detection, investigation, prosecution and punishment of Commonwealth criminal offences. This may include, for example, a member of the public reporting misconduct by a police officer to a more senior officer in the same police force; or reporting to a state oversight body maladministration in the use of information shared by the Commonwealth to a state police force.

Recommendation 29

5.104 The Committee recommends that the Bill be amended to provide for a defence for a person who reports, to an appropriate entity, malpractice or maladministration in the prevention, detection, investigation, prosecution or punishment of a criminal offence against a law of the Commonwealth or the functions of the Australian Federal Police under paragraph 8(1)(be)

---

99 See Australian Broadcasting Corporation, 'The Cabinet Files: How classified documents were found at a Canberra second-hand shop', http://www.abc.net.au/news/about/backstory/news-coverage/2018-02-03/the-cabinet-files-and-how-they-were-found/9393008 viewed 30 April 2018.

of the *Australian Federal Police Act 1979* or the *Proceeds of Crimes Act 2002*.

Defence for legal advice

5.105 The Committee notes concerns that the defences in the Bill do not appear to cover dealing with information for the purpose of seeking legal advice, for example, about the application of the secrecy provisions. The Committee supports the Attorney-General's Department's suggestion that such a defence could be included.

Recommendation 30

5.106 The Committee recommends that the Bill be amended to include a defence for dealing with information for the purpose of obtaining legal advice.

Other matters

Interactions with other legislation

5.107 Participants in the inquiry raised questions about the Bill's interaction with other legislative frameworks, in particular:

- the *Freedom of Information Act 1982* (the FOI Act),
- the *Privacy Act 1988* (the Privacy Act),
- the *Ombudsman Act 1976* (the Ombudsman Act),
- the *Inspector-General of Intelligence and Security Act 1986* (the IGIS Act), and
- the *Public Interest Disclosure Act 2013* (the PID Act).

Interaction with the FOI Act and Privacy Act

5.108 As noted above, the Human Rights Law Centre pointed out in its submission that the breadth of the proposed secrecy offences is such that 'they criminalise the disclosure of information to which Australians have a right to access under the FOI Act'.[100] The Law Council of Australia recommended that the proposed secrecy provisions should expressly

[100] Human Rights Law Centre, *Submission 11*, p. 15.

indicate whether they override the FOI Act and how they will interact with obligations under the Privacy Act.[101]

5.109 The Attorney-General's Department responded that the defences in subsections 122.5(1) (official duties) and subsection 122.5(2) (information made public with the authority of the Commonwealth) will apply if a person is disclosing information under the FOI Act or Privacy Act in the proper performance of his or her functions.[102]

5.110 The Australian Information Commissioner recommended that a note be included in the Bill, or additional information included in the Explanatory Memorandum, to clarify that the secrecy provisions are not intended to impact on Australian Privacy Principle 12 and the Privacy Act, including the Notifiable Data Breaches scheme.[103] The Department responded:

> The department's view is that the secrecy offences do not override these provisions. Indeed, these provisions may be an example of the types of requirements that would indicate that a person's activities were authorised by law or part of their duties (for the purposes of the defences in section 122.5). This could be clarified in the Explanatory Memorandum.[104]

5.111 As discussed above, the Information Commissioner also recommended that a defence similar to that proposed in section 122.5(3) be included in the Bill to cover the communication of information to his office.[105]

Interaction with the Ombudsman Act, IGIS Act and PID Act

5.112 More broadly, the Commonwealth Ombudsman noted that the maximum penalty for an agency staff member failing to comply with a requirement to provide information under section 9 of the Ombudsman Act is three months

---

101 Law Council of Australia, *Submission 5*, p. 71.

102 Attorney-General's Department, *Submission 6.1*, p. 24.

103 Office of the Australian Information Commissioner, *Submission 16*, p. 2.
The Australian Privacy Principles are contained in Schedule 1 to the *Privacy Act 1988*. Australian Privacy Principle 12 states that, subject to certain exceptions, if an entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information.
The Notifiable Data Breaches scheme in Part IIIC of the *Privacy Act 1988* mandates that entities must notify individuals affected by data breaches that are likely to result in serious harm.

104 Attorney-General's Department, *Submission 6.1*, p. 40.

105 Office of the Australian Information Commissioner, *Submission 16.1*, p. 3.

imprisonment or 10 penalty units. In comparison, the maximum penalty for disclosing 'inherently harmful information' in the Bill is 15 years imprisonment. The Ombudsman submitted:

> Agency staff members may find themselves in a dilemma about which piece of legislation has priority and resolve the problem by opting to transgress the provision with the lesser penalty, with the effect that information required by my office to fulfil my functions is not provided.[106]

5.113 The Acting Ombudsman, Ms Jaala Hinchcliffe, expanded on this concern at a public hearing:

> [W]e have a coercive power under section 9 of our act, which enables us to provide in effect a notice to produce documents. We don't usually use that power to obtain information. We usually use our power under section 8, which is a request for information to be provided, but we can use our section 9 power … The point that we're making in our submission is the potential for a Commonwealth official who has been requested to provide documents under that power to be concerned about the potential to commit an offence under these new secrecy provisions in providing that information to us, which has a significantly larger penalty than the penalty in our act for failure to produce.[107]

5.114 The Ombudsman expressed similar concerns in relation to the PID Act, for which he considered the reliance on a defence to a serious offence could discourage the making of disclosures. The Ombudsman supported the inclusion of a provision in the Bill clarifying that the existing immunities in section 24 of the PID Act and sections 7A, 8 and 9 of the Ombudsman Act are not affected.[108]

5.115 Similar concerns were also raised by the IGIS, who suggested the secrecy provisions may override existing immunity provisions in the IGIS Act and PID Act:

> Proposed Division 122 of the Criminal Code does not expressly deal with the interaction of the proposed provisions and existing 'secrecy override' clauses in other legislation, including s 24 of the PID Act and s 18(9) of the IGIS Act. There is a risk that the proposed secrecy offences could be interpreted as overriding such provisions. This would mean that people making PIDs to the

---

106 Commonwealth Ombudsman, *Submission 8*, p. 4.

107 Ms Jaala Hinchcliffe, Acting Commonwealth Ombudsman, *Committee Hansard*, Canberra, 31 January 2018, pp. 3–4.

108 Commonwealth Ombudsman, *Submission 8*, p. 5.

> IGIS and those cooperating with IGIS inquiries could potentially be exposed to criminal liability or at the very least may have doubt about their legal position and concern about the need to rely on the proposed defences with their obligation to discharge the evidential burden. The proposed scheme provide[s] a lesser degree of protection than the immunity from liability that is currently available under s 18(9) of the IGIS Act or s 24 of the PID Act. The reduction of clear legal protections may reduce the willingness of people to provide information to the IGIS.[109]

5.116 The IGIS encouraged the Committee to consider a 'relationship of laws provision' in the Bill to provide that the proposed offences are not intended to override the immunity from liability provisions in the IGIS Act and PID Act.[110]

5.117 Responding to the concerns raised by the IGIS and Ombudsman, the Attorney-General's Department advised:

> The department continues to consider the interaction of the defences and immunities in light of the comments raised by [sic] in the submissions made by the Commonwealth Ombudsman and the IGIS. It may be possible to add a provision to Division 122 to make clear on the face of the Criminal Code that the enactment of the defences is not to be taken as reflecting an intention that they impliedly repeal or otherwise affect any other immunities.[111]

5.118 Alongside proposed amendments to the Bill that were provided to the Committee on 5 March 2018, the Attorney-General indicated that his 'initial view' was that the Bill should be amended by inserting a provision clarifying that that the defences to the secrecy offences in Schedule 2 do not affect any immunities that exist in other legislation.[112] The Attorney-General advised the Committee:

> My view is that it is not necessary to amend the defences in subsections 122.5(3) or (4) so that they are exceptions rather than defences. Consistent with the principles of criminal responsibility in Chapter 2 of the Criminal Code, there is no practical difference between a defence and an exception. The effect of both types of provisions is that a person is not criminally responsible for an offence. Under subsection 13.3(3) of the Criminal Code, a defendant who wishes to rely on any exception, exemption, excuse, qualification or

---

109 Inspector-General of Intelligence and Security, *Submission 13*, p. 4.

110 Inspector-General of Intelligence and Security, *Submission 13*, p. 4.

111 Attorney-General's Department, *Submission 6.1*, pp. 28, 38.

112 Attorney-General, *Submission 40*, p. 4.

> justification provided by the law creating an offence bears an evidential burden in relation to that matter. The evidential burden applies whether a particular matter is framed as a defence or an exception.[113]

5.119 The IGIS expressed her support, in principle, for the Attorney-General's proposal.[114] However, the IGIS commented that 'rules regarding the allocation of evidential burden are not relevant to concerns about the framing of the offences and defences raised in my submission':

> My concern is to eliminate the potential for uncertainty or argument as to whether the offences impliedly abrogate existing immunities and replace them with offence-specific defences. I am also concerned about the non-legal risk that people may be less willing to come forward to IGIS if they must rely upon a defence to a serious criminal offence to do so.[115]

5.120 The IGIS added that, unlike the Ombudsman Act, there is currently no immunity in the IGIS Act for persons who provide information to the office of the IGIS voluntarily outside the PID Act:

> While there are circumstances in which a person who provides information to my Office will be subject to the immunity in section 10 of the PID Act because their communication is a PID, not all persons who disclose information to my Office do so by way of making a PID. This may be because the person is not a 'public official', or because their disclosure does not relate to 'disclosable conduct' by the relevant agency within the meaning of the PID Act, or because the disclosure is not made to an 'authorised officer' under the PID Act.
>
> These persons are currently protected by an absence of applicable criminal offences to their conduct in communicating information to my Office, rather than a positive statutory immunity. The offences in proposed section 122.1 of the Bill will, if enacted in their present form, change this position.[116]

5.121 The IGIS asked that consideration is given to extending the statutory immunities under the IGIS Act to persons who provide information voluntarily, making clear 'preferably by its express terms, an intention for

---

113 Attorney-General, *Submission 40*, p. 5.

114 Inspector-General of Intelligence and Security, *Submission 13.2*, p. 2.

115 Inspector-General of Intelligence and Security, *Submission 13.2*, p. 5.

116 Inspector-General of Intelligence and Security, *Submission 13.2*, p. 6.

the immunity to prevail over laws that would otherwise expose the person to a penalty'.[117]

Penalties

5.122 As outlined in Chapter 4, the proposed secrecy offences relating to communication carry maximum penalties of imprisonment for 15 years, or 20 years for aggravated offences. This contrasts with the existing penalty of two years imprisonment for the equivalent 'official secrets' offence in section 79 of the Crimes Act, or up to seven years if the offence is carried out with an intention to prejudice the security or defence of the Commonwealth. The penalties in the Bill also contrast with the ALRC's recommendation that the maximum penalty for the general secrecy offence be 'seven years imprisonment, a pecuniary penalty not exceeding 420 penalty units, or both'.[118]

5.123 The proposed offences concerning 'other dealings', proper places of custody and lawful directions carry maximum penalties of imprisonment for five years, or 10 years for aggravated offences.

5.124 Some participants in the inquiry considered the penalties proposed in the Bill to be excessive.[119] The Human Rights Law Centre submitted that the 'dramatic increase in penalties' would 'generate a chilling effect across a wide range of matters of public interest':

> If Schedule 2 is passed, a person who handles or discloses information in relation to the Commonwealth government faces the prospect of severe penalties. Even if defences are available, or the information may not be captured, they necessarily face the uncertainty of how the law would apply to them, and whether arrest and prosecution may proceed. The regime in Schedule 2 is focused exclusively on deterring the disclosure of government information. It is not in keeping with the values of open government, and

---

117 Inspector-General of Intelligence and Security, *Submission 13.2*, pp. 6–7.

118 Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, Report 112, December 2009, p. 262.

119 Joint media organisations, *Submission 9*, p. 7; Australian Lawyers for Human Rights, *Submission 7.1*, p. 2; Human Rights Law Centre, *Submission 11*, pp. 19-20; *Submission 11.2*, p. 6; Mr Edward Santow, Human Rights Commissioner, *Committee Hansard*, Canberra, 31 January 2018, p. 48; Joint councils for civil liberties, *Submission 31*, pp. 15-16.

> encouraging Commonwealth employees to understand government information as ordinarily public information, except in select circumstances.[120]

5.125 The Centre also noted the 'wide range' of disciplinary or employment based sanctions that could be applied to government employees engaged in the unauthorised disclosure of information.[121]

5.126 The Explanatory Memorandum states that the maximum penalty for communication of information 'needs to be adequate to deter and punish a worst case offence'. In the case of communication of information causing harm to Australia's interests, the Explanatory Memorandum states that the worst case offence could include the 'communication of official information with the intent of compromising a major law enforcement or national security investigation, or that results in the death of, or serious injury to, a large number of people'. For communication of inherently harmful information, the Explanatory Memorandum states that the worst case offence could include 'intentional or corrupt disclosures of inherently harmful information, and disclosures that may irreparably damage the defence or security of Australia for decades'.[122]

5.127 The Law Council of Australia recommended that, in the absence of an express harm requirement, the secrecy offences should cascade in penalty and require that a person knew, or as a lesser offence, was reckless as to whether, the protected information falls within a particular category.[123] The Human Rights Law Centre similarly suggested that offences could be staggered so that disclosures occasioning loss of life had more severe maximum penalties than other disclosures.[124]

---

120 Human Rights Law Centre, *Submission 11*, pp. 19–20.

121 Human Rights Law Centre, *Submission 11*, p. 8.

122 Explanatory Memorandum, p. 255.

123 Law Council of Australia, *Submission 5*, p. 57; *Submission 5.1*, p. 2; Dr Natasha Molt, Deputy Director of Policy, Policy Division, Law Council of Australia, *Committee Hansard*, Melbourne, 16 March 2018, p. 12.

124 Dr Aruna Sathanapally, Director of Legal Advocacy, Human Rights Law Centre, *Committee Hansard*, Melbourne, 16 March 2018, p. 23.

Attorney-General's consent to institute proceedings

5.128 The Bill does not propose requiring the Attorney-General's consent for prosecutions of the secrecy offences in Schedule 2. This is in contrast to the existing 'official secrets' offences in section 79 of the Crimes Act.

5.129 The proposed secrecy offences also contrast with the proposed offences for espionage, theft of trade secrets, foreign interference, sabotage and other threats against security in Schedule 1 to the Bill, all of which contain a consent requirement. In relation to those offences, the Attorney-General's Department described the requirement for Attorney-General's consent for prosecutions as a 'further safeguard'. It noted:

> 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.[125]

5.130 The Committe asked the Department why the Attorney-General's consent was not proposed to be required for secrecy-related prosecutions. The Department responded:

> The Attorney-General's consent is commonly required to commence proceedings that could affect Australia's international relations or national security. These are considerations that the Commonwealth Director of Public Prosecutions is not able to take into account under the Prosecution Policy of the Commonwealth.
>
> Such provisions provide the Attorney-General with an opportunity to receive advice from relevant agencies and other Ministers on sensitivities that might arise if proceedings are commenced for offences, and provides opportunity for consideration of whether the prosecution could be detrimental to Australia's foreign relations and national security.
>
> Secrecy offences do not inherently raise such considerations.[126]

---

125 Attorney-General's Department, *Submission 6*, p. 49.

126 Attorney-General's Department, *Submission 6.1*, p. 68.

5.131 The prosecution policy of the Commonwealth states:

> There are a variety of reasons for the inclusion of such consent requirements in legislation, but all are basically intended to ensure that prosecutions are not brought in inappropriate circumstances.
>
> … In some cases the consent provision will have been included as it was not possible to define the offence so precisely that it covered the mischief aimed at and no more. Other cases may involve a use of the criminal law in sensitive or controversial areas, or must take account of important considerations of public policy. In appropriate cases the decision whether to consent to a prosecution is made after consultation with a relevant department or agency.[127]

5.132 In its 2009 report, the ALRC considered the question of whether the Attorney-General's consent should be required for prosecutions under the general secrecy offence. A requirement for the Attorney-General's consent appeared to be supported by the Attorney-General's Department and the Australian Intelligence Community at the time. However, the ALRC did not recommended including such a requirement, citing concerns that it had previously raised about the political nature of consent requirements in the context of sedition laws.[128]

Consequential amendments

Telecommunications interception

5.133 Under Schedule 4 to the Bill, discussed in Chapter 10, enforcement agencies will be able to apply for a telecommunications interception warrant for the purpose of investigating any of the secrecy offences in the Bill. Currently, telecommunications interception warrants are only generally available in relation to secrecy offences carrying a penalty of imprisonment for seven years for more.

Citizenship applications

5.134 Under consequential amendments discussed in Chapter 10, all of the secrecy offences in the Bill will be part of the definition of 'national security offences' in the *Australian Citizenship Act 2007* for which the Minister is obliged to

---

127 Commonwealth Director of Public Prosecutions, *Prosecution Policy of the Commonwealth*, p. 8.

128 Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, Report 112, December 2009, pp. 264–268.

refuse certain citizenship applications made by stateless persons. Currently this obligation only applies to the 'official secrets' provisions in section 79 of the *Crimes Act*, and not the unauthorised disclosures offences in section 70 (which are replicated in proposed section 122.4).

Committee Comment

Interaction with other legislation

5.135 The Committee notes the Attorney-General's Department's evidence that there is no intention for the secrecy provisions to override the obligations and immunities that exist in other legislation. The Committee considers there is scope for further clarity to be included in the Bill on the relationship between these laws.

5.136 In relation to the IGIS Act, the Committee notes that, unlike in the Ombudsman Act, there is currently no immunity for persons who provide information to the IGIS office voluntarily and outside of the PID Act. As the Bill introduces serious criminal offences that capture a broad range of dealings with Commonwealth information, the Committee supports the existing immunities in the IGIS Act being extended to cover the voluntary provision of information.

Recommendation 31

5.137 The Committee recommends that the Bill be amended to clarify that the secrecy offences in Schedule 2 do not override the obligations and immunities included in the:

- ***Freedom of Information Act 1982*,**
- ***Privacy Act 1988*,**
- ***Ombudsman Act 1976*,**
- ***Inspector-General of Intelligence and Security Act 1986*, or**
- ***Public Interest Disclosure Act 2013*.**

Recommendation 32

5.138 The Committee recommends that the *Inspector-General of Intelligence and Security Act 1986* be amended to extend statutory immunity to persons who voluntarily provide information to the Inspector-General or her office.

Attorney-General's consent

5.139 The Committee notes that, unlike other offences in the Bill, it is not proposed that the Attorney-General's consent be obtained prior to the commencement of a prosecution under the secrecy offences. This is in line with the recommendation of the ALRC.

5.140 However, the Committee notes that the ALRC's recommendation was in the context of a narrower set of secrecy offences, which extended only to unauthorised communication of information by Commonwealth officers and included harm-based requirements in all instances. The Committee considers that, noting the broader range of information and conduct captured by the Bill, and its application to all persons, it is appropriate that the Attorney-General be required to consent to any prosecution and consider the applicable defences. Noting the potential for highly sensitive cases to arise, including in relation to journalists and national security matters, this additional layer of scrutiny may help to guard against impacts on freedom of expression.

Recommendation 33

5.141 The Committee recommends that Bill be amended to require the Attorney General's consent for a prosecution under the proposed secrecy offences in Division 122 of the Bill. In deciding whether to consent, the Attorney-General should be required to consider whether the conduct might have been authorised or is otherwise covered by an exception under any of the proposed defences in the Division.

Penalties

5.142 The Committee notes that the unauthorised disclosure of certain types of information held by the Commonwealth can have very serious implications including, in extreme cases, long term damage to Australia's security and the safety of a large number of people. While in most cases the damage is

likely to be less extreme, it is appropriate that the maximum penalties in the Bill be serious enough to deter these type of disclosures.

5.143 The Committee considers that the maximum penalties for the communication offences should be reduced to seven years' imprisonment, consistent with the ALRC's recommendation. As a result, the penalties for the dealing offences should also be reduced to three years' imprisonment, to maintain the current structure of the secrecy offences, which impose a higher maximum penalty for offences involving the communication of information than for offences relating to other dealings. The maximum penalties for the aggravated communications offences, in section 122.3, should be reduced to 10 years' imprisonment. This would align with the maximum penalties for the communications offences in the *Intelligence Services Act 2001*. The maximum penalties for the aggravated dealing offences should be reduced to five years' imprisonment.

Recommendation 34

5.144 Consistent with recommendations of the Australian Law Reform Commission, the Committee recommends that the Bill be amended to reduce the maximum penalty for the secrecy offences in proposed sections 122.1, 122.2 and 122.4A to seven years' imprisonment for conduct involving communication of information, and three years' imprisonment for other dealings.

The maximum penalty for the aggravated secrecy offences in proposed section 122.3 should be ten years' imprisonment for conduct involving communication of information (consistent with the most serious secrecy offences in the *Australian Security Intelligence Organisation Act 1979* and the *Intelligence Services Act 2001*), and five years' for other dealings.

6. Espionage offences

6.1 This chapter discusses the new espionage offences proposed in Schedule 1 to the Bill.

6.2 The proposed espionage offences were a discussed by a range of participants in the Committee's inquiry, with concerns centring on the breadth of conduct captured by the offences, the limitations posed to freedom of expression and political communication and the limited available defences.

6.3 During the course of the inquiry the Attorney-General proposed amendments to some provisions in the Bill affecting the espionage offences. This chapter considers the espionage offences both as outlined in the Bill, and taking into account the Attorney-General's proposed amendments.

6.4 This chapter considers

- the rationale for the proposed new offences,
- evidence concerning the breadth of conduct captured by the offences,
- evidence concerning the offence-specific defences available in relation to the offences, and
- other matters, including penalties and interactions with other legislation.

Overview of the provisions

6.5 Schedule 1 will amend Part 5.2 of the Criminal Code to replace current espionage laws. The Bill will repeal the four current espionage offences in Division 91, replacing these with 35 offences overall: 10 underlying offences and 25 aggravated offences.

6.6 The new offences and proposed penalties are set out below.

Table 6.1 Espionage offences

Offence	Section	Penalty	Aggravated offences
Subdivision A - Espionage			
Espionage—dealing with information etc. concerning national security which is or will be made available to foreign principal - intention as to national security	91.1(1)	Life	91.6(b) (i)–(v)
Espionage—dealing with information etc. concerning national security which is or will be made available to foreign principal - reckless as to national security	91.1(2)	25 years	91.6(b)(i)–(v)
Espionage—dealing with information etc. which is or will be made available to foreign principal - intention as to national security	91.2(1)	25 years	91.6(b)(i)–(v)
Espionage—dealing with information etc. which is or will be made available to foreign principal - reckless as to national security	91.2(2)	20 years	91.6(b)(i)–(v)
Espionage—security classified information etc.	91.3	20 years	91.6(b)(i)–(v)
Subdivision B – Espionage on behalf of foreign principal			
Espionage on behalf of foreign principal - intention as to national security	91.8(1)	25 years	N/A
Espionage on behalf of foreign principal - reckless as to national security	91.8(2)	20 years	N/A
Espionage on behalf of foreign principal - conduct on behalf of foreign principal	91.8(3)	15 years	N/A
Subdivision C—Espionage-related offences			

Offence	Section	Penalty	Aggravated offences
Offence of soliciting or procuring an espionage offence or making it easier to do so	91.11	15 years	N/A
Offence of preparing for an espionage offence	91.12	15 years	N/A

*If the penalty for the underlying offence is imprisonment for 25 years, the penalty for the aggravated offence will be imprisonment for life. If the penalty for the underlying offences is 20 years, the penalty for the aggravated offence will be imprisonment for 25 years.

Rationale for the proposed new offences

6.7 Existing espionage offences in Division 91 of the Criminal Code concern conduct that does, will or is intended to, make certain information or articles available to a foreign country, a foreign organisation, or person acting on their behalf. Currently, espionage laws are limited to information 'concerning the Commonwealth's security or defence', or 'concerning the security or defence of another country', but only where the information was acquired by the Commonwealth.[1]

6.8 The Director-General of Security described the changing nature of modern espionage as follows:

> espionage now ranges from its classical form of a foreign spy typically paying an official for classified information and then using tradecraft to conceal that act—early John Le Carre stuff, if you like—to what is now complex cyberintrusion that's conducted typically from overseas to enable the theft of sensitive technologies. The wonder of cyberintrusion is that it's comparatively cheap, it's instantaneous and, most importantly, it's very difficult to detect and to attribute.[2]

6.9 The Attorney-General's Department explained in its submission the need to reform existing laws, which is considered to be insufficient in the following ways:

---

1 Refer to paragraphs 91.1(1)(a), 91.1(2)(a) and 91.1(3)(a) of the *Criminal Code*.

2 Mr Duncan Lewis, Director-General of Security, Australian Security Intelligence Organisations, *Committee Hansard*, Melbourne, 16 March 2018, p. 33.

- offences are limited to intentional conduct: offences only cover conduct where a person intends to prejudice Australia's security or defence, or to advantage the security or defence of a foreign country.
- offences are limited to security or defence information: the disclosure of this information 'represents the most serious end of the offending spectrum', however, the communication of other information, such as information held outside the Commonwealth by private contractors, academic institutions or political organisations can be equally damaging.
- prosecution is required to prove an absence of 'lawful authority': where the offence relates to conduct intended to advantage the security or defence of a foreign country, the prosecution must prove beyond reasonable double that the communication was made without lawful authority. This is said to be a significant barrier to prosecution, especially where the subject of prosecution is a current or former Commonwealth officer.
- current espionage laws do not take account of contemporary methodologies: current espionage laws cover communicating information or making, obtaining or copying a record. This does not sufficiently reflect technological advances, such as the evolving sophistication and complexity of cyber-attacks.[3]

6.10 Some of the key differences between the existing espionage offences and the proposed new offences in the Bill include:

- some proposed offences do not require the offender to intend to prejudice national security, with some using the lower threshold of 'reckless' and others requiring neither intention nor recklessness,[4]
- the proposed espionage offences will not be limited to information concerning security or defence. Some proposed offences will require that the information is security classified or 'concerns Australia's national security'; for other offences, any information or article could form the basis of an espionage charge,[5]
- the conduct will relate to 'foreign principals', a term defined in the Bill to include a broader range of foreign organisations and actors,[6]

---

3 Attorney-General's Department, *Submission 6*, pp. 9-10.

4 Proposed sections 91.1(2), 91.2(2), 91.3, and related offences in proposed section 91.6, 91.8(3), 91.11 and 91.12.

5 Proposed section 91.2.

6 Proposed section 90.2

- lack of lawful authority is not an element in any of the proposed offences,
- the Bill criminalises preparing, planning, soliciting and procuring espionage,
- the Bill introduces a range of aggravated offences, and
- the maximum penalty is increased from 25 years imprisonment to imprisonment for life.

6.11 A number of submitters did not support the proposed reforms to the proposed espionage offences, and some submitters expressed serious concerns.[7] This chapter will discuss the specific concerns of participants. The Committee also received a large number of form letters from members of the public raising concerns regarding the proposed espionage offences.[8]

Subdivision A – Espionage

6.12 All five espionage offences proposed in Subdivision A (and the 25 related aggravated offences) are premised on a person engaging in conduct that results or will result in information or an article being made available to a foreign principal. The offences are distinguished by two variables: the character of the information or article; and the person's intent (if any) at the time of committing the offence. These variables can be summarised as follows:

Table 6.2 Division 91, Subdivision A - Espionage

Section	Type of information/article	Intention/recklessness
91.1(1)	Has a security classification or 'concerns' Australia's national security	Intent to prejudice Australia's national security or advantage the national security of a foreign country
91.1(2)	Has a security classification	Reckless as to whether conduct

7 Law Council of Australia, *Submission 5*, p. 46; Australian Lawyers for Human Rights, *Submission 7*; Joint media organisations, *Submission 9*; Human Rights Watch, *Submission 10*; Human Rights Law Centre, *Submission 11*; Australian Lawyers Alliance, *Submission 12*; Valerie Heath, *Submission 14*; Australian Human Rights Commission, *Submission 17*; Centre for Media Transition, *Submission 23*; Joint councils for civil liberties, *Submission 31*, p. 56; GetUp Australia, *Submission 38*, p. 2; WWF-Australia, *Submission 36*, p. 1.

8 *Submissions 45 to 49*.

	or 'concerns' Australia's national security	will prejudice Australia's national security or advantage the national security of a foreign country
91.2(1)	Any	Intent to prejudice Australia's national security
91.2(2)	Any	Reckless as to whether conduct will prejudice Australia's national security
91.3	Has a security classification or 'concerns' Australia's national security	No intent or recklessness as to national security required.

6.13 The scope of espionage offences rests upon the interpretation of key concepts, namely:

- the types of information that the Bill captures,
- the conduct that the Bill captures by 'dealing' with information,
- the required fault elements, including the meaning of 'prejudicial to national security', and
- the meaning of 'making information available to a foreign principal'.

6.14 Many participants in the inquiry raised concerns about the breadth of conduct captured by the proposed espionage offences. Submitters expressed concern that a broad range of benign and public interest conduct would be captured by the offences, in particular citing operations of human rights groups, think tanks, consultants, journalists, universities, Australia's allies, lawyers, and private citizens as being potentially affected.[9] Specific concerns raised by participants are discussed below.

6.15 The Attorney-General's Department responded:

> The expansion of the scope of the espionage offences is necessary in order to cover the full range of espionage conduct being engaged in by Australia's foreign adversaries.[10]

[9] For example, Law Council of Australia, *Submission 5*, p. 45.

[10] Attorney-General's Department, *Submission 6.1*, p. 12.

Meaning of 'made available' to a foreign principal

6.16 Both current and proposed espionage offences relate to conduct which results in information or articles being 'made available' to foreign entities.

6.17 The Bill does not define the term 'made available' exhaustively. However, the Dictionary to the Criminal Code states:

> [M]ake available, in relation to material, includes, but is not limited to, describing how to obtain access, or describing methods that are likely to facilitate access, to material (for example: by setting out the name of a website, an IP address, a URL, a password, or the name of a newsgroup).[11]

6.18 The Explanatory Memorandum does not address the meaning of 'made available' in the context of the proposed espionage offences. However, proposed section 90.1 defines the term 'deal' to include a similar phrase: 'makes it available'. In this context, the Explanatory Memorandum states:

> 'Makes it available' is intended to cover the passage of information or articles *other than by disclosing or publishing it*. This is intended to cover situations where arrangements are made between two individuals to pass information using a pre-arranged location, without the individuals needing to meet.[12] (emphasis added)

6.19 The espionage offences require that the person has 'made available' the information to a foreign principal or person acting on behalf of a foreign principal. However, the Bill does not require a person to have in mind a particular foreign principal, and the person may have in mind more than one foreign principal.[13]

6.20 Accordingly, the joint media organisations argued that communicating information online, in print, or by broadcast would breach the espionage provisions.[14] Similarly, Human Rights Watch submitted:

> [I]t is not clear how strong the causative link needs to be between a person's conduct and information becoming available to a foreign principal. For

---

11 *Criminal Code*, Dictionary; Section 90.1 of the *Criminal Code* defines 'article' to include 'material'. The *Criminal Code* Dictionary does not define 'material'. A limited definition of 'material' as it applies to Part 10.6 of the *Criminal Code* provides that material includes material in any form, or combination of forms, capable of constituting a communication.

12 Explanatory Memorandum, p. 96.

13 Proposed subsections 91.1(5); 91.2(3); 91.3(2); 91.8(4)-(5); and 91.11(2).

14 Joint media organisations, *Submission 9*, p. 7-8; Human Rights Watch; *Submission 10*, pp. 2, 4.

> example, the new offences may apply to users of social media who share leaked information by reposting it on Facebook or Twitter. Similarly, sections 91.1(2), 91.2(2) and 91.3 may in effect criminalise the publication of politically sensitive information that a foreign principal may independently access.[15]

6.21 The Attorney-General's Department confirmed that with regard to the espionage offence in proposed section 91.1, 'it is possible that the information could be communicated to a foreign principal through publication of news', but noted that the offence in section 91.1 can only be established if the person was aware of a substantial risk that his or her conduct would prejudice Australia's national security or advantage the national security of a foreign country and, having regard to the circumstances known to him or her, it is unjustifiable to take the risk'.[16] The Attorney-General's Department also confirmed that the espionage offences could cover privately, professionally or commercially produced research, opinions, advice or analysis made available to foreign principals.[17]

6.22 Upon questioning from the Committee, the Attorney-General's Department considered that defining the term 'makes available' in the Bill was not necessary.[18] The Attorney-General's Department acknowledged that 'a person can deal with information by publishing it online'.[19]

Breadth of definitions of 'national security' 'foreign principal' and 'deals'

6.23 The definitions of 'national security' and 'foreign principal', as used across the Bill, are discussed in Chapter 3. This chapter focuses on the use of these terms, in addition to the term 'deals', in the context of the proposed espionage offences.

6.24 Current espionage offences criminalise making certain information available to a foreign country, foreign organisation, or person acting on behalf of a foreign country or foreign organisation. The *Criminal Code* does not define the term 'foreign organisation'.

---

15 Human Rights Watch, *Submission 10*, p. 4-5.

16 Attorney-General's Department, *Submission 6.1*, p. 34.

17 Attorney-General's Department, *Submission 6.1*, p. 68.

18 Attorney-General's Department, *Submission 6.1*, p. 70.

19 Attorney-General's Department, *Submission 6.1*, p. 70.

6.25 The Bill replaces the current, undefined terms of 'another country or a foreign organisation' and 'a person acting on behalf of such a country or organisation' with a new concept of a 'foreign principal' or persons acting on behalf of a foreign principal. The term 'foreign principal' is defined in proposed section 90.2.

6.26 Existing espionage offences only relate to information that concerns 'security or defence.'[20] A number of the new espionage offences rely upon the proposed new definition of 'national security' in section 90.4.

6.27 Current espionage offences criminalise 'communicating or making available' information. In contrast, the proposed espionage offences require a person to 'deal' with information, which is broadly defined in proposed section 90.1 to include receiving, obtaining, collecting, possessing, making a record of, copying, altering, concealing, communicating, publishing or making available.

6.28 The Explanatory Memorandum highlights a key distinction between the current and proposed offences:

> The new offences criminalise a broad range of dealings with information, including possessing or receiving, and protect a broader range of information, including unclassified material. The current methodology of Australia's adversaries means that dealings with unclassified information, if accompanied by the requisite intention to harm Australia, can be as damaging as the passage of classified information. The new offences will not just target the person who discloses the information, but also the actions of the foreign principal who receives the information. The new offences in Division 91 will also, for the first time, criminalise soliciting or procuring a person to engage in espionage and will introduce a new preparation or planning offence, which will allow law enforcement agencies to intervene at an earlier stage to prevent harmful conduct occurring.[21]

6.29 Submitters raised concerns that the definitions of national security, foreign principal and deals would interact to significantly expand the scope of espionage laws.[22] The United Nations Special Rapporteurs submitted that 'adopting such a sweeping definition' of national security would broaden

---

20 *Criminal Code*, section 91.1.

21 Explanatory Memorandum, p. 26.

22 WWF-Australia, *Submission 36,* p. 1; GetUp, *Submission 38*, pp. 1-2; Joint councils for civil liberties, *Submission 31*, p. 56.

the scope of the espionage offences 'while conferring far-reaching discretion on the government.'[23]

6.30 Human Rights Watch submitted that the intersection between the definition of 'foreign principal' and 'national security' would likely capture legitimate collaboration with international organisations, for example,

> [h]uman rights activists and organizations meet regularly with foreign diplomats, United Nations representatives and regional groups like ASEAN and the European Union to raise concerns about abusive governmental policies and press for change.[24]

6.31 Similarly, the Australian Lawyers Alliance and Human Rights Watch raised concerns that the breadth of the proposed definitions of 'deal' and 'national security' would 'dramatically expand the nature of the activities to which the [espionage] provisions will apply, when compared with the existing rules' and make the ambit of what is considered 'espionage' extremely broad.[25]

6.32 The Law Council also argued that the definitions of 'national security' and 'foreign principal' are defined so broadly, that the proposed espionage offences go 'far beyond' existing laws:

> Part of the problem comes from the wide definition of 'national security' … particularly, the elements of political relations with another country … Another aspect is how this broad definition applies to the definition of a foreign principal … which covers state owned companies (and enterprises that are directed or controlled by the state) and foreign private companies that are being used to channel government activities.
>
> The proposed espionage offences, with the economic and political elements of the definition of national security, would seem to cover any form of consultancy with a foreign government, the sort that accountancy or legal firms may engage in as a matter of course. It may also cover the provision of

---

23 United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; and the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism; and the Special Rapporteur on the situation of human rights defenders, *Submission 30*, p. 7.

24 Human Rights Watch, *Submission 10*, p. 5.

25 Australian Lawyers Alliance, *Submission 12*, pp. 5, 10; Human Rights Watch, *Submission 10*, p. 5.

> information to other entities such as foreign banks or state owned companies by Australian companies or businesses.[26]

6.33 The Law Council submitted that these broad definitions could also capture journalists, academics, consultants, individual citizens and allies.[27] The Law Council submitted that Australian think tanks or advocacy groups that provide information to a 'foreign principal' may also be caught.[28] GetUp shared this view, submitting that its activities were likely to be affected. GetUp submitted that the proposed espionage offences would capture

> instances in which Australian breaches of international law are communicated to an international body, such as the United Nations or an international news organisation.[29]

6.34 The Committee received a large number of form letters from members of the public expressing similar concerns that the espionage laws could inhibit journalists, whistle-blowers and activists from holding the government to account.[30]

6.35 GetUp also submitted that the extended definition of 'national security' would capture harm caused to Australia's international reputation, which would have a practical effect 'upon GetUp's campaigning on issues such as the Trans-Pacific Partnership, refugees and climate change.'[31] Accordingly, GetUp recommended that the definition of 'foreign principal' be limited to foreign governments and their agents.[32] A number of form letters received by the Committee similarly raised concerns that the laws could be used to avoid government embarrassment.[33]

6.36 Citing concerns that the espionage laws could be used to obscure embarrassing, illegal, corrupt or otherwise damaging government conduct, the Australian Lawyers Alliance advocated an alternative approach:

---

26 Law Council of Australia, *Submission 5*, p. 46.

27 Law Council of Australia, *Submission 5*, p. 47.

28 Law Council of Australia, *Submission 5*, p. 46.

29 GetUp, *Submission 38*, p. 2.

30 See for example *Submissions 45 to 49*.

31 GetUp, *Submission 38,* p. 2.

32 GetUp, *Submission 38,* p. 2.

33 *Submissions 46*.

> Concepts of espionage and the definitions that underpin it must be limited to the work of intelligence services, and not expanded to allow the traditional operations of government to be obscured.[34]

6.37 GetUp similarly recommended limiting the scope of offences to acts that compromise Australia's security or defence.[35]

Breadth of information captured

6.38 The espionage offences in proposed sections 91.1 and 91.3 (and related offences)[36] apply to information and articles which:

- 'concern' Australia's national security; or
- have a security classification.

6.39 The espionage offences in proposed section 91.2 (and related offences)[37] apply to *any* article or information.

6.40 'Information' is defined to include information of any kind, whether true or false, whether in material form or not, and including an opinion or a report of a conversation.[38] An 'article' includes any thing, substance or material.[39] The Bill proposes that for the purposes of Division 91, 'dealing with information or an article' will include dealing with part of the information or article; or the substance, effect or description of the information or article.[40]

---

34 Australian Lawyers Alliance, *Submission 12*, p. 7.

35 GetUp, *Submission 38,* p. 3.

36 Proposed section 91.6 (aggravated espionage offences); proposed section 91.8 (espionage on behalf of foreign principal), proposed section 91.11 (offence of soliciting or procuring an espionage offence or making it easier to do so); and proposed section 91.12 (offence of preparing for an espionage offence).

37 Proposed section 91.6 (aggravated espionage offences); proposed section 91.8 (espionage on behalf of foreign principal), proposed section 91.11 (offence of soliciting or procuring an espionage offence or making it easier to do so); and proposed section 91.12 (offence of preparing for an espionage offence).

38 Criminal Code, s. 90.1

39 *Criminal Code*, section 90.1

40 Proposed section 90.1(2).

Information concerning national security

6.41 The Bill proposes a number of offences that criminalise conduct relating to information that 'concerns Australia's national security'.[41] A number of submitters raised concerns that this threshold lacks clarity.

6.42 The phrase 'concerns' is carried over from the current espionage laws which apply to information 'concerning the Commonwealth's security or defence'.[42] The existing *Criminal Code* does not define the term 'concerns', and neither the Bill nor the Explanatory Memorandum propose to clarify its meaning. Accordingly, the phrase will take its ordinary and natural meaning. The Macquarie Dictionary provides that 'concerns' means 'to relate to; be connected with; be of interest or importance to; affect'.

6.43 For information to 'concern' national security it does not need to have emanated from the Commonwealth Government (or another Australian Government) or that the information was derived from any other sensitive or privileged source. The Attorney-General's Department outlined the rationale for broadening the information to which the espionage offences apply to is that

> 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.[43]

6.44 Submitters identified a number of concerns. The United Nations Special Rapporteurs submitted:

> [T]he lack of specificity regarding information disclosures that will 'prejudice' or 'concern' Australia's national security, or 'advantage' the national security of a foreign country, fails to establish a direct and immediate connection between the expression and the threat. Accordingly, these offences raise the possibility that any person who publicly communicates or receives

---

41 Proposed section 91.6 (aggravated espionage offences); proposed section 91.8 (espionage on behalf of foreign principal), proposed section 91.11 (offence of soliciting or procuring an espionage offence or making it easier to do so); and proposed section 91.12 (offence of preparing for an espionage offence).

42 Criminal Code, section 91.1(1)(a)(i).

43 Attorney-General's Department, *Submission 6*, p. 9.

information deemed politically controversial or sensitive could be prosecuted for espionage.[44]

6.45 Similar concerns were raised by Human Rights Watch and WWF-Australia.[45]

6.46 The Law Council noted as a 'difficulty' that the offences are not limited to sensitive Commonwealth information, but could include situations where information or an article is unclassified material.[46]

6.47 As outlined above, 'national security' is defined broadly to encompass a range of matters beyond the current espionage threshold of 'security or defence'. The Committee questioned whether a private citizen's opinion on Australia's trade, military or political relations could be said to 'concern' Australia's national security. The Attorney-General's Department advised that '[a]lthough it is not possible to give a definitive answer about a hypothetical scenario, the department does not consider it likely that a private citizen's view or opinions on Australia's trade, military or political relations would be information that 'concerns Australia's national security'.[47]

Evidentiary certificates

6.48 The Bill enables the Attorney-General to sign an evidentiary certificate in espionage proceedings. The certificate would be prima facie evidence in proceedings that the information or article in question concerns Australia's national security or concerns a particular aspect of Australia's national security.[48] Several submitters raised concerns regarding the proposed introduction of evidentiary certificates.[49] These matters were discussed in detail in Chapter 3.

---

44 United Nations Special Rapporteurs (on the promotion and protection of the right to freedom of opinion and expression; on the promotion and protection of human rights and fundamental freedoms while countering terrorism; and on the situation of human rights defenders), *Submission 30*, p. 8.

45 Human Rights Watch, *Submission 10*, p. 4; WWF-Australia, *Submission 36*, p. 1.

46 Law Council, *Submission 5*, p. 47.

47 Attorney-General's Department, *Submission 6.1,* p. 68.

48 Schedule 1, item 20 (proposed section 93.3 of the *Criminal Code*)

49 Australian Lawyers Alliance, *Submission 12*, pp. 12–13; Dr Lawrence McNamara, *Submission 19*, p. 2 (in relation to the proposed use of evidentiary certificates in section 122.3)

Security classified information

6.49 The Bill proposes a number of espionage offences, and aggravated espionage offences, that criminalise conduct relating to information or an article that 'has a security classification'.[50]

6.50 Several submitters raised concerns with the introduction of offences premised on dealings with security-classified information.[51] The key issues identified by submitters were:

- the proposal to define the term 'security classification' in regulations,
- the use of an administrative system for document management as the basis of criminal liability, and
- the use of evidentiary certificates and strict liability.

6.51 During the course of the inquiry, the Attorney-General notified the Committee of a number of proposed amendments to the treatment of security classifications in the Bill.[52]

6.52 Submitters' concerns, and the Attorney-General's proposed amendments, are discussed in Chapter 3.

Any information – proposed section 91.2

6.53 In contrast to current espionage offences, the proposed offences at section 91.2 will capture information from any source, on any topic. The offences will arise where a person deals with any article or information and:

- the person intends to prejudice, or is reckless as to whether their conduct will prejudice, 'national security', and
- the conduct results or will result in the information being made available to a foreign principal.

6.54 The Attorney-General's Department submitted that:

> The methodology of Australia's adversaries means that even dealings with unclassified information or publicly available information can be equally as

---

50 Proposed sections 91.1(3); 91.3(3); and 91.6(3). Similar provisions apply to related secrecy offences in proposed Division 122.

51 Law Council of Australia, *Submission 5*, p. 21–24;Human Rights Law Centre, *Submission 11*, pp. 21–22; Inspector-General of Intelligence and Security, *Submission 13*, pp. 7–9; Valerie Heath, *Submission 14*, p. 2; Centre for Media Transition, *Submission 23*, p. 4.

52 Attorney-General, *Submissions 40 and 40.1*.

> damaging to Australia's national security interests as dealings with classified information.[53]

6.55 The Explanatory Memorandum contains the following example:

> Person A is a Commonwealth official employed as an analyst at a government department. Person A is strongly opposed to Australia's intention to negotiate a treaty with Country B. Person A compiles a report informed by the knowledge he has gained through his role as an analyst in the government department, which contains an aggregation of sensitive, but publically available, information—informed by expertise Person A has developed as a government analyst. Person A provides this to an official of Country B with the intention of convincing Country B not to negotiate the treaty with Australia, thereby harming Australia's international relations.[54]

6.56 Some submitters were concerned that the information would not need to derive from a sensitive source or relate to national security, and could include unclassified material.[55] In light of the preceding discussion, a range of online activity could be seen to satisfy this threshold.

6.57 The Attorney-General's Department confirmed that proposed section 91.2 could cover privately, professionally or commercially produced research, opinions, advice or analysis, and 'applies to any information and does not require it to be security classified or concern national security'.[56]

6.58 The Department also noted that the existing espionage offences in the Criminal Code are not limited to information originating from government.[57] The existing offences apply to information concerning:

- the Commonwealth's security or defence, and
- the security or defence of another country, being information that the person acquired from the Commonwealth.

6.59 Existing section 90.1 defines 'security or defence' of a country to include the operations, capabilities and technologies of, and methods and sources used by, the country's intelligence or security agencies.

---

53 Attorney-General's Department, *Submission 6*, p. 14.

54 Explanatory Memorandum, *p. 115.*

55 Law Council, *Submission 5*, p. 47; Human Rights Watch, *Submission 10*, p. 4.

56 Attorney-General's Department, *Submission 6.1*, p. 68.

57 Attorney-General's Department, *Submission 6.1*, p. 68.

6.60 Human Rights Watch recommended restricting espionage offences to information that has a security classification and concerns national security.[58] This would require removing the proposed section 91.2 from the Bill and modifying proposed sections 91.1 and 91.3.

6.61 The Law Council of Australia recommended that, in the event that the espionage offences proceed, the offences should be limited to 'Commonwealth information'.[59] The Attorney-General's Department responded:

> The effect of this amendment would be to significantly limit the application of espionage offences only to Commonwealth officers and people who received information from a Commonwealth officer. This limitation is not present in existing offences relating to information about the Commonwealth's security and defence and its introduction [would] undermine the protection of Australia's interests.
>
> The amendments seek to broaden the offences to cover the information being sought by Australia's foreign adversaries. Espionage activity is not limited to seeking information held by, or received from, a Commonwealth officer.[60]

Fault elements

6.62 The Bill introduce three tiers of espionage offences:

- offences which require the person to intend their conduct to prejudice Australia's national security (or in some instances advantage the national security of a foreign country),
- offences which require the person to be reckless as to whether their conduct will prejudice Australia's national security (or in some instances advantage the national security of a foreign country), and
- offences which do not require any intention or recklessness as to national security.

---

58 Human Rights Watch, *Submission 10*, p. 2.

59 This would be defined as information a person had access to by virtue of being or having been a Commonwealth officer, or information provided to the person by a Commonwealth officer. Law Council of Australia, *Submission 5*, p. 49.

60 Attorney-General's Department, *Submission 6.1*, p. 12.

Prejudice Australia's national security

6.63 A number of the proposed espionage, sabotage and foreign interference offences require a person to engage in conduct either with a recklessness as to whether their conduct will 'prejudice' Australia's national security, or an intention to prejudice Australia's national security. Chapter 3 discusses the term, as used across the Bill.

6.64 Submitters were concerned that this threshold would capture a broad range of conduct under the umbrella of 'espionage'.[61] GetUp raised concerns that this threshold would be met by damaging Australia's reputation, and submitted that persons should be free to protest and criticise government, regardless of the impact on the Australian Government's reputation overseas.[62]

6.65 As noted in Chapter 3, the Attorney-General's Department advised that the reference to 'political and economic relationships' in the definition of national security would extend to a government's reputation or relationships with a foreign government, or between officials.[63]

Recklessness to national security

6.66 In contrast to current espionage laws, a number of the proposed espionage offences will capture offences committed with the less culpable mental state of 'recklessness' regarding national security.

6.67 A person is reckless with respect to a result if the person is aware of a substantial risk that the result will occur and having regard to the circumstances known to them, it is unjustifiable to take the risk.[64]

6.68 The Attorney-General's Department submitted that:

> 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.

---

61 Human Rights Watch, *Submission 10,* p. 5; GetUp, *Submission 38*, p. 2.

62 GetUp, *Submission 38*, pp. 2, 3.

63 Attorney-General's Department, *Submission 6.1*, p. 45.

64 *Criminal Code*, section 5.4.

> … 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.[65]

6.69 A number of submissions raised concerns with the introduction of reckless espionage offences.[66] The joint media organisations anticipated that a reckless offence could capture legitimate journalism, providing:

> Section 91.1(2) provides the offence for recklessly dealing with information prejudicial to Australia's national security in a way that makes it available to a foreign power. It would be the case that communicating such information online, in print, or by broadcast would breach the provision. Further, to breach this section a journalist or media organisation would not need to have a foreign power in mind.
>
> We note that the only applicable defence is that the information was already in the public domain with the authority of the Commonwealth.[67]

Offences which do not require the offender to consider national security

6.70 One of the key changes proposed by the Bill is the introduction of espionage offences that do not require the offender to intend, or even be reckless as to whether their conduct would or could prejudice Australia's national security or advantage the national security of a foreign country.

6.71 In this third tier, the prosecution will not need to prove that the person had any awareness that their conduct could prejudice Australia's national security, or benefit another country. These offences omit the element found in other espionage offences that requires the prosecution to prove that the person possessed some intention or recklessness as to national security. The relevant offences are:

---

65 Attorney-General's Department, *Submission 6*, p. 15.

66 Joint media organisations, *Submission 9*, p. 8; Human Rights Watch, *Submission 10*, p. 2; Australian Lawyers Alliance, *Submission 12*, p. 10.

67 Joint media organisations, *Submission 9*, p. 8. The joint media organisations' concerns could apply equally to the reckless offence set out in section 91.2(2), or to the offence in section 91.3, which does not require either an intention to prejudice national security or recklessness as to national security.

- the offence in proposed section 91.3, which can arise where a person makes information available to a foreign principal, and that information concerns Australia's national security or has a security classification. It is not an element of the offence that the person intended to prejudice national security, or was reckless to it.
- the aggravated offences arising from the underlying offence in proposed section 91.3, which similarly do not require recklessness or intention to national security.
- the offence in section 91.8(3), which requires that a person deals with information or an article; is reckless as to whether their conduct involves the commission by another person of an espionage offence; and engages in the conduct in connection with a foreign principal. In contrast to the offences set out in sections 91.8(1) and 91.8(2) it is not an element of the offence that the person engaged in this conduct intending to prejudice national security, or being reckless as to whether their conduct would prejudice national security.
- flowing from the offences in proposed section 91.3 and 91.8, the ancillary offences in proposed sections 91.11 and 91.12, which similarly do not require an intent or recklessness as to national security.

6.72 Human Rights Watch submitted that all espionage offences should contain an element that requires the person to intend to cause harm.[68]

6.73 The Law Council similarly submitted that the espionage offences should require (as a minimum for 'outsiders') that the dealing with the information did, or was reasonably likely to, or intended to prejudice Australia's national security or advantage the national security of a foreign country.[69]

Extra-territoriality and sovereignty

6.74 Both the current and proposed espionage offences will be subject to extended geographical jurisdiction (category D). This means that the offence is available where:

- the conduct and the result of the alleged offence occur outside Australia,
- the person engaged in the conduct is not an Australian citizen or resident, and

---

68 Human Rights Watch, *Submission 10*, p. 2.

69 Law Council of Australia, *Submission 5*, p. 49.

- the conduct is lawful in the country in which it is committed.[70]

6.75 The Explanatory Memorandum provides that:

> Category D geographical jurisdiction is appropriate because intelligence agencies may undertake key facets of espionage activities against Australia in foreign countries to conceal these activities from hostile authorities. [71]

6.76 However, the offences as drafted will also capture conduct that foreign actors undertake within their own country in order to advance their national interest. For example, the offence in proposed section 91.2 will be made out where a person (regardless of their location or nationality) makes information or an article available to a foreign principal, reckless as to whether this conduct would prejudice Australia's national security. Given the broad definition of national security, and the intended meaning of 'prejudice' (discussed above), a broad range of activity undertaken by sovereign states could be captured. For example, if a foreign public official provided internal briefing documents to their government, in order to negotiate trade deals or treaties with Australia, this would likely satisfy both the offences in proposed sections 91.2 and 91.3.

6.77 The Criminal Code would require the Attorney-General's consent to prosecute such a charge, but the person could be arrested, charged or remanded on bail before such consent was obtained.[72]

Aggravated offences

6.78 The Bill proposes creating a number of aggravated espionage offences that will apply where a person commits an offence against proposed Subdivision A.

Table 6.3 Aggravated espionage offences

An aggravated offence will arise where a person commits one of the underlying offences in Subdivision A and any of the following circumstances exist in relation to the commission of the underlying offence:	
91.6(1)(b)(i)	the person dealt with information or an article that has a

[70] Proposed sections 91.7, 91.10 and 91.14; and *Criminal Code* , section 15.4.

[71] Explanatory Memorandum, pp. 134, 148, and 159.

[72] *Criminal Code*, sect ion 16.1.

	security classification of SECRET or above;
91.6(1)(b)(ii)	the person dealt with information or an article from a foreign intelligence agency;
91.6(1)(b)(iii)	the person dealt with 5 or more records or articles each of which has a security classification;
91.6(1)(b)(iv)	the person altered a record or article to remove or conceal its security classification;
91.6(1)(b)(v)	at the time the person dealt with the information or article, the person held an Australian Government security clearance.

6.79 The effect of committing an aggravated espionage offences is:

- if the penalty for the underlying offences is 20 years, the penalty for the aggravated offence will be imprisonment for 25 years.
- if the penalty for the underlying offence is imprisonment for 25 years, the penalty for the aggravated offence will be imprisonment for life.[73]
- where the underlying offence carries a maximum penalty of life imprisonment, the aggravating conduct will be taken into account in determining the sentence (proposed section 91.5).

6.80 A number of the key terms in the aggravated offences' are not defined, including:

- 'security classification' in proposed subsections 91.6(1)(b)(i), (iii) and (iv);
- 'secret or above' in proposed subsection 91.6 (1)(b)(i); and
- Australian Government security clearance in subsection 91.6 (1)(b)(v).

6.81 The aggravated espionage offences are similar to the aggravated offences created in the context of the secrecy provisions. The issues affecting both provisions are discussed in Chapter 3.

6.82 The Law Council of Australia submitted that the problems with the underlying offences are exacerbated by the existence of the proposed aggravated offence. The Council pointed to the drafting of the provisions which

[73] Proposed section 91.6(1).

> does not require that the person knows that the: information or an article has a security classification of secret or above; that the information is from a foreign intelligence agency; that the 5 or more records or articles had a security classification.[74]

Government proposed amendments

6.83 On 13 February 2018, the Attorney-General's Department advised the Committee that it had been asked by the Attorney-General to progress a number of changes to the Bill. Draft amendments were provided by the Attorney-General on 5 March 2018. As discussed in Chapter 3, the proposed amendments affecting the espionage offences included:

- amending proposed section 90.5, which defines security classification, to mean a classification of SECRET or TOP SECRET, or any other equivalent classification or marking prescribed by the regulations,
- removing subsections 91.1(3) and 91.6(3), which apply strict liability on whether information or articles have a security classification, and
- removing an aggravated espionage offence where the person deals with information or an article that has security classification of SECRET or above.[75]

6.84 The proposed amendments also make significant changes to the espionage offence at proposed section 91.3, which does not require the person to intend that, or be reckless as to whether, their conduct will prejudice Australia's national security. The amendments propose including an additional element that

> (aa) the person deals with the information or article for the primary purpose of making the information or article available to a foreign principal or a person acting on behalf of a foreign principal.[76]

6.85 The Attorney-General explained:

> The inclusion of this additional element ensures that the offence will not inappropriately cover the publication of information by a journalist whose

---

74 Law Council of Australia, *Submission 5*, pp. 47–48.

75 Attorney-General, *Submission 40.1*.

76 Attorney-General, *Submission 40.1*, p. 1.

conduct does indirectly make the information available to a foreign principal, but whose primary purpose is to report news or current affairs to the public.[77]

6.86 The amended section 91.3 would also no longer apply to information or AN article that 'concerns Australia's national security'—that is, it would only apply in relation to security classified information.[78]

6.87 Submitters generally viewed the proposed amendments to section 91.3 positively.[79] The joint councils for civil liberties, for example, described the changes as a 'significant improvement'.[80]

6.88 The Law Council of Australia noted that the addition of the proposed 'primary purpose' element would 'still leave a person providing information about oil and gas negotiations with East Timor to the Timorese Government or a United Nations Agency liable to the offence'. However, the Law Council acknowledged that (depending on how liberally security classifications are imposed) such negotiations may not attract the SECRET or TOP SECRET classification required for the conduct to constitute an offence.[81]

Subdivision B – Espionage on behalf of foreign principal

6.89 Proposed Subdivision B creates three new offences of 'espionage on behalf of foreign principal' (proposed section 91.8). An offence arises where a person:

- engages in conduct on behalf of, directed, funded or supervised by a foreign principal, and
- the person is reckless as to whether the conduct involves the commission by any person of an offence against Subdivision A, and
- the person:
  - intends to prejudice Australia's national security or advantage the national security of a foreign country (proposed section 91.8(1)), or

77 Attorney-General, *Submission 40*, p. 4.

78 Attorney-General, *Submission 40.1*, p. 2.

79 Law Council of Australia, *Submission 5.1*, p. 3; Human Rights Law Centre, *Submission 11.2*, p. 1; Joint councils for civil liberties, *Submission 31.1*, p.4.

80 Joint councils for civil liberties, *Submission 31.1*, p.4.

81 Law Council of Australia, *Submission 5.1*, p. 3.

- is reckless as to whether their conduct will prejudice Australia's national security or advantage the national security of a foreign country (proposed section 91.8(2)), or
- neither intends nor is reckless as to national security (proposed section 91.8(3)).

6.90 The issues relating to the Subdivision A offences (discussed above) apply equally to the offences proposed in Subdivision B. In addition, the Law Council raised particular concerns relating to proposed section 91.8. The Law Council submitted that a person could be convicted of an offence under proposed section 91.8:

> … subject to a 25 or 20 year imprisonment term for dealing with information or an article which may come under the definition of 'national security' in a way that they intend to advantage for example a foreign client which may be a state owned company and guilty of an offence if they are reckless as to whether any other person engages in an espionage offence.[82]

6.91 The Law Council raised particular concerns with the proposed offence in section 91.8(3):

> Under proposed subsection 91.8(3) there is no requirement even that the person intended or was reckless as to whether their conduct will prejudice Australia's 'national security' or advantage the 'national security' of a foreign country. A person may be subject to a term of imprisonment for 15 years.[83]

Subdivision C – Espionage-related offences

6.92 Proposed Subdivision C creates two new espionage offences:

- soliciting or procuring an espionage offence or making it easier to do, and
- preparing for an espionage offence.

6.93 The offences in Subdivision C are ancillary offences to the offences set out in Subdivision A and Subdivision B of Division 91. Accordingly, the concerns raised by submitters in relation to the Subdivision A and B offences (discussed above) are equally applicable to Subdivision C offences. In addition, submitters raised additional concerns pertaining specifically to the Subdivision C offences.

---

82 Law Council of Australia, *Submission 5*, p. 48.

83 Law Council of Australia, *Submission 5*, p. 48.

Soliciting, procuring and making it easier to commit espionage

6.94 Proposed section 91.11 will make it an offence for a person acting on behalf of, in collaboration with, directed, funded or supervised by a foreign principal or person acting on their behalf to solicit, procure, or 'make it easier' for another person to undertake espionage. The Explanatory Memorandum provides:

> The purpose of this offence is to address gaps in the current law, which does not criminalise soliciting or procuring espionage. This offence will give law enforcement the means to deal with this conduct at the time it occurs, without the need to wait until an espionage offence is committed or sensitive information is actually passed to a foreign principal.[84]

6.95 The Explanatory Memorandum also provides that these offences are intended to

> accommodate for the wide range of activity and techniques that the practice of soliciting or procuring espionage encompasses. It is possible that when the offender makes contact with a target the offender will not have particular information or a thing, or a particular kind of dealing with the information or thing, in mind. For example, the offender may only know that the target is well connected to government or that the target has access to classified information, without knowing exactly what information the target can provide. Further, there is no fixed pattern for how an offender will approach a target. In some instances the offender will meet the target and solicit information in one dealing. In other instances, the offender may build a relationship of trust with the target through multiple dealings, and intends to build up to inducing the target to commit espionage.[85]

6.96 The phrase 'procure' is defined in the Dictionary to the Criminal Code insofar as it relates to procuring a person to engage in sexual activity. In this context procure includes conduct to:

a. encourage, entice or recruit the person to engage in that activity; or

b. induce the person (whether by threats, promises or otherwise) to engage in that activity.

---

84 Explanatory Memorandum, p. 149.

85 Explanatory Memorandum, p. 152.

6.97 It is intended section 91.11 will be interpreted consistently with this definition.[86]

6.98 The term 'solicits' is not defined and will take its ordinary meaning. The Explanatory Memorandum provides that this is intended to include asking for, requesting, pressing for, or trying to obtain information or a thing from another person.[87]

6.99 'Making it easier' is also not defined. The Explanatory Memorandum provides that the term is intended to capture

> behaviour such as cultivating or grooming a target before the attempt to solicit or procure espionage is made. For example, a person may arrange meetings, provide gifts, or seek to establish a relationship of trust or friendship with a target. It would also include seeking passage of an unclassified government document or informed comment with the intent of procuring or soliciting the target to provide classified information in the future.[88]

6.100 A number of submitters criticised this proposed offence.[89] The Law Council raised concerns that the ambiguity of the terms 'making it easier' would extend the already broad scope of the offences, and that this offence was so broad that it could capture

> a foreign government or state owned company (a client) that seeks to establish a relationship with an Australian economist or range of consultancy services (who is not a Commonwealth officer or Australian Government employee) for the purpose of obtaining information regarding what Australian companies may be worth investing in.[90]

6.101 Human Rights Watch was concerned that, consistently with other espionage offences, no intention to harm is required.[91]

6.102 The Law Council submitted that the offence is not needed in light of the availability of offences for attempt under existing section 11.1 of the *Criminal Code*.[92]

---

86 Explanatory Memorandum, p. 151.

87 Explanatory Memorandum, p. 150.

88 Explanatory Memorandum, p. 151.

89 Law Council of Australia, *Submission 5*, p. 48; Human Rights Watch, *Submission 10*, p. 4-5.

90 Law Council of Australia, *Submission 5*, p. 48.

91 Human Rights Watch, *Submission 10*, p. 4.

Preparing for espionage

6.103 Proposed section 91.12 will introduce an offence for preparing for or planning an offence of espionage (proposed subdivision A), or espionage on behalf of a foreign principal (proposed subdivision B).

6.104 The Explanatory Memorandum states that the purpose of the proposed offence is to

> give law enforcement authorities the means to deal with preparatory conduct and enable a person to be arrested before any [sic] without the need to wait until an espionage offence is committed or sensitive information is actually passed to a foreign principal.[93]

6.105 The Bill does not define the terms 'preparation' and 'planning'. The Explanatory Memorandum provides that these terms are intended to take their ordinary meanings, but provides the following examples of conduct which could satisfy the proposed offences:

- the term 'preparation' could include acts to conceive, formulate, make ready, arrange, and assemble an idea, plan, thing, or person for an offence against Subdivision A (espionage) or B (espionage on behalf of foreign principals).
- the term 'planning' could include acts to organise, arrange, design, draft, or setup an idea, plan, thing, or person for an offence against Subdivision A (espionage) or B (espionage on behalf of foreign principals).[94]

6.106 General issues concerning the Bill's inclusion of preparatory offences are discussed in Chapter 3.

Defences

6.107 The general defences available under Part 2.3 of the Criminal Code will apply to the proposed espionage offences. Additionally, the Bill proposes four specific defences:

- dealing in accordance with a law of the Commonwealth,[95]

---

92 Law Council of Australia, *Submission 5*, p. 48.

93 Explanatory Memorandum, p. 153.

94 Explanatory Memorandum, p. 154.

95 Proposed sections 91.4(1)(a); 91.9(1)(a); and 91.13(1)(a).

- dealing in accordance with an arrangement or agreement allowing exchange of information, to which the Commonwealth is a party,[96]
- dealings in the person's capacity as a public official,[97] and
- dealings in information that has already been communicated or made available to the public with the authority of the Commonwealth (available for all offences other than those outlined in Subdivision C).[98]

6.108 Some of these defences are also available in proceedings for the proposed foreign interference and secrecy offences, and are considered in detail in those chapters (see Chapter 5 and 7).[99] A number of additional defences exist for the proposed secrecy offences, for example, the defence of prior publication and the defence of fair and accurate reporting.[100]

6.109 Some submitters raised concerns that the defences proposed in the Bill are insufficient.[101]

6.110 For example, the Law Council of Australia considered the application of the defence, dealing with information 'in accordance with a law of the Commonwealth', was unclear for circumstances where a defendant is unable to point to a specific law of the Commonwealth that they were acting in accordance with.[102] The Attorney-General's Department considered that Commonwealth officers would not have difficulty describing where they thought that authority arose.[103] Chapter 3 discusses the effect of the evidential burden being placed on the defendant in relation to defences.

---

96 Proposed sections 91.4(1)(b); 91.9(1)(b); and 91.13(1)(b).

97 Proposed sections 91.4(1)(c); 91.9(1)(c); and 91.13(1)(c).

98 Proposed sections 91.4(2) and 91.9(2).

99 The following defences are available for foreign interference offences: engaging in conduct in accordance with a law of the Commonwealth; in accordance with an arrangement or agreement to which the Commonwealth is party; or in the person's capacity as a public official (proposed ss. 92.5 and 92.11). The following defences are available for secrecy offences: dealings in accordance with an arrangement or agreement to which the Commonwealth is party; dealings in the person's capacity as a public official; and dealings in information that has already been communicated with the consent of the Commonwealth (proposed ss. 122.5(1)(a); 122.5(1)(b) and 122.5(2)).

100 Proposed sections 122.5(8) and 122.5(6).

101 Law Council of Australia, *Submission 5*, p. 48; GetUp, *Submission 38*, p. 3.

102 Law Council of Australia, *Submission 5*, pp. 46–47.

103 Attorney-General's Department, *Submission 6.1*, p. 52.

6.111 A number of submitters recommended that a defence of prior publication should be available for espionage offences.[104] In relation to the proposed secrecy offences, proposed subsection 122.5(8) contains a defence for 'prior publication', which refers to information that has already been communicated, or made available to the public. The Attorney-General's Department argued that an equivalent prior publication defence is not appropriate for espionage offences, noting that proposed sections 91.1 and 91.2 include the element that the person intended to, or was reckless as to whether his or her conduct would, prejudice Australia's national security (or advantage the national security of a foreign country).[105]

6.112 A number of submitters also raised concerns regarding the absence of a public interest defence.[106] In contrast to the secrecy offences, the Bill does not provide any defence for journalists or news reporting.

6.113 The Australian Lawyers Alliance submitted that, given the broad scope of the proposed espionage offences, the lack of a public interest defence would be likely to 'stifle essential public interest disclosures'.[107] The Alliance cited the publication of the Panama Papers, Paradise Papers and the Nauru Files as prosecutable conduct under the proposed espionage offences.[108]

6.114 The joint media organisations recommended that a general public interest defence or journalist defence be made available for all espionage and secrecy offences, on the basis that 'this is the only way to ensure public interest reporting can continue and Australians are informed of what is going on in their country'.[109] Human Rights Watch made a similar recommendation.[110] The joint media organisations submitted that the risk 'that a journalist could

---

104 Law Council of Australia, *Submission 5*, p. 49; Joint Media Organisations, *Submission 9*, p. 8, Australian Lawyers for Human Rights, *Submission 7*, pp. 2–3.

105 Attorney-General's Department, *Submission 6.1*, p. 72.

106 Australian Lawyers Alliance, *Submission 12*, p. 12; Human Rights Law Centre, *Submission 11*, p. 11; *Submission 11.2*, pp. 7-8; Human Rights Watch, *Submission 10*, p. 2 and 5; Valerie Heath, *Submission 14*, p. 1; GetUp, *Submission 38, p. 3.*

107 Australian Lawyers Alliance, *Submission 12*, p. 12.

108 Australian Lawyers Alliance, *Submission 12*, p. 11.

109 Joint media organisations, *Submission 9*, p. 1.

110 Human Rights Watch, *Submission 10*, p. 3.

go to jail for doing their job is very real, and as a result of reporting in the public interest'.[111]

6.115 GetUp agreed that journalists should be protected but stressed that 'robust exemptions' should be introduced 'to protect not just journalists, but all citizens' protesting or raising evidence of wrongdoing against the Australian Government.[112]

6.116 The Attorney-General's Department did not agree that it would possible for the conduct captured by the espionage offense to be 'in the public interest':

> It is hard to see how the passage of information to a foreign principal could be in the public interest where it is done with an intention to, or reckless as to whether the person's conduct will, prejudice Australia's national security or advantage the national security of a foreign country. The espionage offences (other than section 91.3) require proof of this element.[113]

6.117 The Law Council of Australia also recommended introducing defences to capture and protect bona fide business dealings and persons acting in good faith, for example, consultants and professionals acting in their ordinary capacity.[114]

6.118 The Attorney-General's Department argued otherwise:

> A bona fide dealings or good faith defence is not appropriate in the context of espionage offences which (with the exception of section 91.3) require proof of a person's intention or recklessness as to whether their conduct will prejudice Australia's national security or advantage the national security of a foreign country … It is difficult to conceive a situation in which a person could simultaneously be reckless as to harming Australia's national interest, yet be acting in good faith. Genuine good faith would preclude recklessness being made out.[115]

Exposure to liability – public officials and allies

6.119 The Explanatory Memorandum provides that the espionage offences

---

111 Joint media organisations, *Submission 9*, p. 8.

112 GetUp, *Submission 38, p. 3.*

113 Attorney-General's Department, *Submission 6.2*, p. 3; Attorney-General's Department, *Submission 6.1*, p. 28.

114 Law Council of Australia, *Submission 5*, p. 48.

115 Attorney-General's Department, *Submission 6.2*, p. 2; Attorney-General's Department, *Submission 6.1*, p. 14.

> are only intended to apply where a person's dealing with information is not a proper or legitimate part of their work. There are a vast range of legitimate circumstances in which public officials deal with information concerning Australia's national security (including highly classified information) in performing their duties. For example, possessing or copying information concerning national security is a day to day occurrence in many Commonwealth departments and agencies and for Ministers and their staff. It is not intended to criminalise these dealings.[116]

6.120 Consistent with the existing espionage offences in the *Criminal Code*, however, a range of proper and legitimate work will be caught by the espionage offences. This is because a number of the offences do not require harm, or an intention or recklessness as to prejudice national security (as discussed above). Similar to the existing references to 'another country or a foreign organisation' in the current espionage offences, the Bill's definition of 'foreign principal' does not distinguish between friend and foe.

6.121 The espionage offences as drafted will capture legitimate government business, including intelligence sharing with foreign allies and partner agencies. At present, officials must generally rely on the defence of 'lawful authority' in section 10.5 of the *Criminal Code* to undertake work that would otherwise be captured by the espionage offences. As the Explanatory Memorandum notes, this defence

> is narrow and only applies to conduct that is specifically justified or excused by a law. Consistent with the definition of law in the Dictionary to the *Criminal Code*, this means the conduct must be specifically justified or excused by a law of the Commonwealth, and includes the *Criminal Code*.[117]

6.122 The Bill introduces a series of new, broader defences for officials, permitting them to deal with information

a. 'in accordance' with a law of the Commonwealth, rather than the law of the Commonwealth needing to specifically justify or excuse the person's conduct,

b. 'in accordance with an arrangement or agreement to which the Commonwealth is party and which allows for the exchange of

---

116 Explanatory Memorandum, p. 144.

117 Explanatory Memorandum, p. 123.

information or articles, such as an intelligence sharing agreement or arrangement with a foreign partner,[118]

c. in their capacity as a public official.

6.123 The Bill as drafted will require the Commonwealth staff undertaking these roles to rely upon a statutory defence in order to undertake their routine duties—that is, that the conduct was undertaken in their capacity as a public official, in accordance with a Commonwealth arrangement or otherwise in accordance with law.[119] Staff will bear the evidentiary burden for their defence.

6.124 This issue is discussed in more detail in Chapter 3, and is also discussed in Chapter 5 in relation to the secrecy offences. In relation to the secrecy offences, a number of submitters referred to the comprehensive review of secrecy laws undertaken by the Australia Law Reform Commission (ALRC) in 2009. The ALRC review did not consider espionage offences, but in relation to secrecy offences the Commission recommended that there should be exceptions (as opposed to defences) in the general secrecy offence for disclosure in the course of an officer's functions or duties; disclosure with the authority of an agency head or minister; and disclosure of information that is already lawfully in the public domain.[120]

Consistency with secrecy defences

6.125 The Human Rights Law Centre noted that much of the conduct captured by the secrecy offences (discussed in Chapter 4) 'could equally be captured by some of the other provisions'.[121] The Centre noted the importance of ensuring that defences across the secrecy and espionage offences are consistent, in order to ensure that:

> … the weakness of safeguards in one regime does not compromise the other by allowing for an alternative avenue for the prosecution of disclosure in the public interest.[122]

---

118 Explanatory Memorandum, p. 124.

119 Proposed sections 91.4, 91.9, and 91.13.

120 Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, Report 112, December 2009, p. 24.

121 Dr Aruna Satahanapally, Director of Legal Advocacy, Human Rights Law Centre, *Committee Hansard*, Melbourne, 16 March 2018, p. 24.

122 Human Rights Law Centre, *Submission 11*, p. 11.

Penalties

Proportionality

6.126 The Bill proposes increasing the maximum penalty for an espionage offence from 25 years to life imprisonment. A number of new espionage offences, such as 'reckless' espionage will carry the same penalty as the current espionage offence, which requires an intent to cause harm.

6.127 The Attorney-General's Department advised:

> 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.
>
> 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.[123]

6.128 Some submitters raised concerns about the severity of the proposed penalties.[124] The law firm Nyman Gibson Miralis submitted that these penalties are disproportionate because the offences do not require harm to be caused.[125] The firm submitted that:

---

123 Attorney-General's Department, *Submission 6*, p. 12.

124 Law Council of Australia, *Submission 5,* pp. 12 and 49; Human Rights Law Centre, *Submission 11*, p. 19; Nyman Gibson Miralis, *Submission 35,* p. 4; WWF Australia, *Submission 36,* p. 2.

125 Nyman Gibson Miralis, *Submission 35,* p. 4.

> Though criminal sentencing is a discretionary exercise, the exceptionally wide range of conduct captured by the proposed espionage offences could create too much uncertainty and lack of consistency in sentencing decisions.[126]

6.129 The firm recommended making amendments to section 16A of the *Crimes Act 1914*—which concerns the matters to which court to have regard when passing sentence—to address this.[127]

Freedom of political communication and expression

6.130 Flowing from the intersection of the various issues discussed above, submitters outlined a broad range of benign, legitimate and public interest conduct that could be captured by the espionage offences.[128] In this context, a number of submitters were concerned that these laws would infringe the right to freedom of expression, and the implied right to political communication.[129] The United Nations Special Rapporteurs submitted:

> We are gravely concerned that the Bill would impose draconian criminal penalties on expression and access to information that is central to public debate and accountability in a democratic society.[130]

6.131 However, the Explanatory Memorandum's Statement of Compatibility with Human Rights does not address whether the right to freedom of expression would be restricted by the proposed espionage offences. The Statement's consideration in this regard is limited to inciting mutiny and secrecy offences.[131]

6.132 Consistent with the criticisms made of the secrecy provisions, some submitters considered that the proposed espionage laws would have a

---

126 Nyman Gibson Miralis, *Submission 35,* p. 4.

127 Nyman Gibson Miralis, *Submission 35,* p. 4.

128 Nyman Gibson Miralis, *Submission 35,* p. 4.

129 Law Council of Australia, *Submission 5*; Human Rights Watch, *Submission 10*; Australian Lawyers Alliance, *Submission 12;* Australian Human Rights Commission, *Submission 17,* p. 1 (the Commission's submission was limited to the proposed secrecy laws, but noted the content of the submission would also apply to the proposed espionage provisions); United Nations Special Rapporteurs, *Submission 30,* p. 2; Get Up Australia, *Submission 38*, p. 1.

130 United Nations Special Rapporteurs, *Submission 30,* p. 2.

131 Explanatory Memorandum, p. 20.

'chilling effect' on political discourse,[132] and could operate to prevent government from being held to account.[133] The Committee also received a large number of form letters from members of the public raising concerns regarding the Bill's 'chilling effect' on freedom of expression. Form letters also expressed concern that the Bill would silence critics of the government and impact journalists, activists and whistle-blowers.[134]

6.133 The Law Council submitted that the proposed espionage offences may not be compatible with, and could have a stifling effect on, freedom of expression.[135] The joint civil liberties councils submitted that the proposed laws would 'inevitably stifle our democracy'.[136]

6.134 The Parliamentary Joint Committee on Human Rights, in its review of the Bill, commented:

> For a measure to be a proportionate limitation on the right to freedom of expression it must be sufficiently circumscribed. In this respect, it appears that the offences as drafted capture a very broad range of conduct. For example, under the offence of dealing with security classified information under proposed section 91.3, it appears that a journalist, by publishing any information subject to a security classification online, will commit an offence. This is because online publication would necessarily make the information available to a foreign principal. Noting that a large number of government documents may be defined as security classified, the extent of the limitation on the right to freedom of expression imposed by these offences is extensive Further, it would appear to still be an offence for a journalist in the above example even if the information were unclassified if it concerned 'Australia's national security'.[137]

6.135 The Law Council also questioned the constitutionality of the proposed espionage laws:

---

132 Law Council of Australia, *Submission 5*, p. 18 United Nations Special Rapporteurs, *Submission 30,* p. 2; Valerie Heath, *Submission 14*, p. 1; WWF-Australia, *Submission 36*, p. 1.

133 Valerie Heath, *Submission 14*, p. 1.

134 See for example *Submissions 45 to 49*.

135 Law Council of Australia, *Submission 5,* pp. 18; 46.

136 Law Council of Australia, *Submission 5*, p. 46; GetUp, *Submission 38,* p. 3; Joint councils for civil liberties, *Submission 31*, p. 36.

137 Parliamentary Joint Committee on Human Rights, *Human rights scrutiny report (Report 2 of 2018)*, pp. 19–20.

> Primarily, the Law Council is concerned that Australians, Australian businesses and advocacy groups and journalists may be caught by the offences for innocuous conduct that is undertaken as a matter of course or in the public interest. In circumstances where the dealing with the information or article relates to politics, and specifically elections, a question may also arise as to whether the provisions will be read down by a court so as to avoid invalidity with the implied right to freedom of political communication.[138]

6.136 The Law Council expanded:

> In circumstances where reporting on politics occurs for example regarding Australia's elections and the reporting results or will result in the information or article being made available to a foreign principal or a person acting on behalf of a foreign principal, a question arises as to the extent that this may be inconsistent with the implied right to freedom of political communication. The current and proposed checks and balances may not be sufficient to ameliorate this concern.[139]

6.137 The Australian Lawyers Alliance submitted that it was particularly concerned about the ramification that the Bill would have for freedom of speech in Australia (in respect of both the proposed secrecy offences and espionage offences).[140] Pointing to complexities in establishing standing in constitutional challenges, the Australian Lawyers Alliance noted that the provisions could possibly operate despite constitutional invalidity, for want of legal challenge.[141] In light of this potentiality, the Alliance recommended:

> … the Bill should be reformed to ensure that all communication of a political nature, including that which might be embarrassing for the government or MPs, is not prohibited by its proposed provisions.[142]

---

138 Law Council of Australia, *Submission 5*, p. 45. The Council referred to *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520; *Australian Capital Television Pty Ltd and New South Wales v Commonwealth* (1992) 177 CLR 106; and *Nationwide News Pty Ltd v Wills* (1992) 177 CLR 1.

139 Law Council of Australia, *Submission 5*, p. 47. The Council referred to the Commonwealth Director of Public Prosecutions, *Prosecution Policy of the Commonwealth* (2014); and proposed section 93.1 which would require the Attorney-General's consent prior to the institution of the proceedings against a person for an offence against Part 5.2.

140 Australian Lawyers Alliance, *Submission 12*, p. 17.

141 Australian Lawyers Alliance, *Submission 12*, p. 18.

142 Australian Lawyers Alliance, *Submission 12*, p. 19.

6.138 The Australian Lawyers Alliance submitted that an adequate explanation had not been provided for the expanded scope of activities which would be captured as espionage, but that in any event

> [c]oncepts of espionage and the definitions that underpin it must be limited to the work of intelligence services, and not expanded to allow the traditional operations of government to be obscured. It should never prevent or prohibit exposure of information that reveals wrongdoing, corruption, or other matters of public interest. Revealing such information ultimately strengthens national security, and the legislation should not inhibit it. Government must always be open and accountable, unless there are clear and persuasive arguments for secrecy, and in those cases any secrecy must be limited to those matters for which it is justified and absolutely essential.[143]

6.139 Professor Rory Medcalf, of the Australian National University's National Security College, submitted in relation to the package of Bills that

> … on the whole the Bills reflect the kind of legislation Australia urgently needs to protect its national security from what ASIO has identified as an unprecedented set of threats of foreign interference and influence. At the same time, the Bills need suitable and early refinement to ensure they reflect a consistent respect for freedom of expression.[144]

6.140 Professor Medcalf submitted:

> Refinements to the present Bills should be possible to limit such perceived or actual collateral harm, such as the rights of academics transparently to conduct international dialogues and research collaboration and the rights of professional journalists to protect their sources and to report on national security issues in the public interest.[145]

Attorney-General's Consent

6.141 In contrast to the proposed secrecy offences, the consent of the Attorney-General will be required to institute proceedings. Proposed section 93.1 requires the consent of the Attorney-General to be granted before instituting proceedings, however, a person may be detained, arrested and placed on remand before this time. Human Rights Watch submitted that the

---

143 Australian Lawyers Alliance, *Submission 12*, p. 7.

144 Professor Rory Medcalf, *Submission 33*, pp. 10–11.

145 Professor Rory Medcalf, *Submission 33*, p. 10.

requirement to obtain the consent of the Attorney-General does not sufficiently mitigate the threat to liberty that the espionage offences carry.[146]

Consequential amendments

Citizenship

6.142 The Bill proposes expanding the current citizenship cessation regime to include all of the new espionage offences proposed by the Bill. The Bill also proposes that a conviction for any of these offences will be grounds to refuse the citizenship application of a stateless person. This is discussed in Chapter 10.

Presumption against bail

6.143 The Bill proposes applying a presumption against bail to all espionage offences where it is alleged that the person's conduct caused, or carried a substantial risk or causing the death of a person. This is discussed in Chapter 10.

Standard non-parole periods

6.144 The Bill proposes requiring minimum non-parole periods to be fixed in relation to all of the new proposed espionage offences. This is discussed in Chapter 10.

Committee Comment

6.145 As outlined in Chapter 1, the Committee seeks to ensure that each of the measures in the Bill is:

- clear and unambiguous in its terms,
- proportional and appropriately targeted to the threat, and
- enforceable.

6.146 The Committee accepts that there is a pressing need to reform Australia's espionage laws in order to reflect the full range of malicious conduct that could harm Australia's national security. The Director-General of Security gave frank evidence that foreign intelligence services can and do adapt how they conduct espionage in Australia so as to exploit gaps in our legal framework. As such, the Committee accepts that it is necessary to ensure

146 Human Rights Watch, *Submission 10,* p. 5.

that the espionage offences apply to the full range of conduct that those foreign intelligence services, their agencies and their proxies engage in, when seeking to obtain classified, sensitive and privileged information to harm Australia's interests, and to further the interests of their own country. However, these interests cannot and should not displace the requirement for clarity and proportionality in the law, as outlined above.

6.147 A number of the proposed espionage offences have been drafted broadly, to ensure that they capture the fully array of means by which foreign intelligence services commit espionage in Australia. The Committee accepts that the Government has, in fact, sought to bring greater clarity to the scope of the proposed new espionage offences compared with the existing offences in the Criminal Code. Nevertheless, the breadth of the proposed new offences may come at the cost of the scope of these offences being uncertain. The effect of this uncertainty is particularly acute due to the espionage offences' intersection with the right to freedom of expression and the implied right of political communication. Imprecise laws may have a broad unintended effect of deterring the democratic communication of political ideas and the operation of a free press, due to fear of prosecution. The gravity of the penalties (life imprisonment and loss of citizenship) may further compound this deterrent effect. This has the potential to go beyond the intention of discouraging malicious insiders and foreign actors from undermining our national security.

6.148 Accordingly, the Committee has made a number of recommendations refining the proposed espionage offences to provide greater certainty and more effectively target the need to protect information that could harm Australia's national security if disclosed.

6.149 The Committee notes that certain offences proposed in the Bill apply to dealings with information that is either security classified or 'concerns national security'. The term 'concerns national security' is not defined in either the existing *Criminal Code* or the Bill, however the existing espionage offences in section 91.1 of the *Criminal Code* include a similar term 'information concerning the Commonwealth's security or defence'. Both the existing term, and the proposed new term, cover classified information and 'official' Commonwealth Government information, as well as sensitive information derived from other sources. Espionage is not, and has never been, universally concerned with access to 'official' or 'secret' information. For example, there are countless historical examples of persons committing

espionage during wartime by observing the publicly-visible movements of warships and forces, and passing information about those movements to an enemy power. The existing espionage offences in the *Criminal Code*, and those in the laws of many comparable jurisdictions, do not include such a limit.

6.150 Nevertheless, in seeking to criminalise those who commit espionage by collecting sensitive and privileged, but non-secret information to harm Australia or advance the interests of a foreign power, the Bill has the potential to capture legitimate expressions of opinion or other commentary that concerns national security. In relation to most offences, this risk is diminished by the requirement to demonstrate that the person intended, or was reckless as to whether their conduct would harm Australia's national security or advantage the national security of a foreign country. There are certain offences in the Bill for which this is not the case, which are addressed separately below. To address the residual risk, the Committee considers that the Bill should be amended to define the term 'concerns' national security.

Recommendation 35

6.151 The Committee recommends that the Bill be amended to define the term 'concerns' national security.

6.152 The offences in sections 91.1, 91.2 and 91.3 apply not only to the situation where a person commits espionage by directly communicating information to a foreign principal or a person acting on their behalf, but also to the situation where a person makes the information available to the foreign principal or a person acting on their behalf. The Explanatory Memorandum explains that the concept of making information available is intended to capture scenarios such as a person leaving the information in a letterbox for another person to collect at a later date, or giving the information to an intermediary who will later give the information to its intended recipient.

6.153 A more complex case, which was raised in evidence to the Committee, is the case in which a person publishes information, for example, in a book, journal or online. The Committee is conscious that there are numerous, public examples of exceptionally grave harm being caused by the publication of classified or sensitive information—it is plausible that a person would seek to commit espionage by publishing information, if the law permitted them to escape criminal liability by publishing information.

6.154 The Committee acknowledges concerns raised in evidence that certain classes of people, including academics and human rights groups, often publish information relating to Australia's political and economic relations with other countries, in particular. The Committee does not agree that such conduct would ordinarily constitute an offence under the Bill. In the unusual case that such a publication did technically satisfy all of the elements of an offence, the Committee is satisfied that the safeguards contained in the *Prosecution Policy of the Commonwealth* and the Bill would be more than sufficient to prevent an unjust prosecution. In particular, it is unlikely that the Commonwealth Director of Public Prosecutions would consider that prosecuting such a case would be in the public interest. Nor is it likely that the Attorney-General would consent to such a prosecution.

6.155 Nonetheless, some stakeholders have expressed the view that it is unclear whether the term 'made available', as used in the espionage offences, would include making information or a document available by way of publishing it. The Committee considers that the term 'made available' for the purpose of the espionage offences should be defined in the Bill.

Recommendation 36

6.156 The Committee recommends that the Bill be amended to define the term 'made available' for the purpose of the espionage offences.

6.157 Additionally, the Committee considers that a defence should be available such that 'making available' to a foreign principal information that is already in the public domain is not captured by the espionage offences. While the specific drafting of a prior publication defence will require careful consideration, the Committee notes that some of the proposed espionage offences cover similar conduct to the Bill's secrecy offences. It may therefore be appropriate for the new defence to use similar language to proposed section 122.5(8)—'Information that has been previously communicated'.

Recommendation 37

6.158 The Committee recommends that the Bill be amended to introduce a prior publication defence for the proposed espionage offences. The defence should be appropriately drafted to ensure the effectiveness of the provisions whilst protecting freedom of expression and the implied constitutional right to freedom of political communication.

The Bill should further be amended to require that, prior to instituting proceedings to commit a person to trial for an espionage offence, the Attorney-General must consider whether the conduct might be authorised in any of the defences outlined in Division 91.

6.159 As discussed above, a key change proposed by the Bill is the introduction of espionage offences that do not require the offender to intend, or even be reckless as to whether their conduct would or could prejudice Australia's national security or advantage the national security of a foreign country (proposed sections 91.3 and 91.8(3)). As currently drafted, these offences would apply to any dealing with information or an article that is security classified or 'concerns national security', and which makes the information available to a foreign principal (or a person acting on their behalf).

6.160 The Committee notes particular concerns raised in the inquiry about the potential impact of these offences on freedom of expression and political communication. The Committee welcomes the Attorney-General's proposed amendments to section 91.3, which would narrow the scope of the offence to security classified information and information that is dealt with for the 'primary purpose' of making it available to the foreign principal. As discussed in Chapter 3, the Committee also supports the limitation of 'security classified information' to classifications of SECRET or above, and the removal of strict liability from this element of the offence.

Recommendation 38

6.161 The Committee recommends that the Attorney-General's proposed amendments to narrow the scope of the offence in proposed section 91.3 of the Bill be implemented. This includes requiring that the person dealt with the information for the 'primary purpose' of making it available to a foreign principal, limiting the offence to information or articles that have a security classification, and removing strict liability from the offence.

6.162 The Committee notes that proposed sections 91.4 and 91.9 include offence-specific defences for dealings 'in accordance with a law of the Commonwealth'. While existing espionage offences include the absence of lawful authority as an element of the offence, the defendant will bear the evidential burden for the proposed new defence of 'in accordance with a law of the Commonwealth'. Existing section 10.5 of the *Criminal Code* also includes a general defence of 'lawful authority', where the conduct constituting an offence is 'justified or excused by or under a law'. The

Explanatory Memorandum currently includes a brief outline of the legal difference between the defences.[147] However, the Committee considers it would assist in clarifying the scope of the new defence if the Explanatory Memorandum provided examples of situations in which conduct would be excused by the offence-specific defences, but would not be excused by the general defence of lawful authority.

Recommendation 39

6.163 The Committee recommends that the Explanatory Memorandum be amended to clarify the intended scope of the proposed defence in Division 91 for dealings 'in accordance with a law of the Commonwealth'. The Explanatory Memorandum should provide examples of situations in which conduct would be excused by the specific defence, but not the general defence of lawful authority available under section 10.5 of the *Criminal Code*.

6.164 In Chapter 4, the Committee recommended limiting the aggravating factor for the proposed secrecy offences to clearances of Negative Vetting 1 (or equivalent) and above. Negative Vetting 1 is the minimum clearance that enables a person to access SECRET classified material, which, under the Attorney-General's proposed amendments, is the minimum level required for information to be considered having a 'security classification' under the espionage offences. Accordingly, the Committee considers that the aggravating factor for the espionage offences should also be limited to persons holding a clearance of Negative Vetting 1 (or equivalent) and above.

Recommendation 40

6.165 The Committee recommends that the Bill be amended to limit the aggravating factor at subparagraph 91.6(1)(b)(v), in relation to the proposed espionage offences, to persons holding an Australian Government security clearance that allows the person to access information with a classification of SECRET or above.

6.166 The Committee notes the concerns raised by the Law Council of Australia and other submitters regarding the introduction of the offence of preparing for an espionage offence, which displaces the law of attempt. The inclusion

147 Explanatory Memorandum, p. 123.

of preparatory offences in the Bill is discussed in general terms in Chapter 3. In the case of section 91.12, however, the Committee accepts the need for an offence that enables authorities to intervene before a serious espionage offence has been committed. The Committee accepts that existing provisions in the *Criminal Code* may not allow for this in all circumstances.

6.167 As discussed above, the *Statement of Compatibility with Human Rights* in the Explanatory Memorandum does not address whether the right to freedom of expression would be restricted by the proposed espionage offences. The Statement's consideration in this regard is limited to inciting mutiny and secrecy offences. Noting the significant concerns raised by participants about the potential impact of the proposed espionage offences on freedom of expression, the Committee recommends that the *Statement of Compatibility with Human Rights* be updated to explicitly address this matter.

Recommendation 41

6.168 The Committee recommends that the Explanatory Memorandum be amended so that the Statement of Compatibility with Human Rights explicitly addresses the limitation to the right to freedom of expression imposed by the espionage offences.

7. Foreign interference and theft of trade secrets offences

7.1 This chapter discusses the new foreign interference and theft of trade secrets offences proposed in the Bill.

Foreign interference offences

7.2 Schedule 1 to the Bill introduces Division 92 into Part 5.2 of the *Criminal Code*. This Division contains nine new foreign interference offences. Their relevant sections and penalties are set out below:

Table 7.1 Foreign interference offences

Offence	Section	Penalty
Offence of intentional foreign interference – interference generally	92.2(1)	20 years
Offence of intentional foreign interference – interference involving targeted person	92.2(2)	20 years
Offence of reckless foreign interference – interference generally	92.3(1)	15 years
Offence of reckless foreign interference – interference involving targeted person	92.3(2)	15 years
Offence of preparing for a foreign interference offence	92.4	10 years
Knowingly supporting foreign intelligence agency	92.7	15 years

Recklessly supporting foreign intelligence agency	92.8	10 years
Knowingly funding or being funded by foreign intelligence agency	92.9	15 years
Recklessly funding or being funded by foreign intelligence agency	92.10	10 years

7.3 The offences in Subdivision B (92.2—92.4) criminalise a range of conduct undertaken by foreign principals who seek to interfere with Australia's political, governmental or democratic processes, support their own intelligence activities or otherwise prejudice Australia's national security. The offences in Subdivision C (92.7—92.10) target a range of conduct that involves funding, supporting and resourcing of foreign intelligence agencies.

Rationale for the new offences

7.4 The Explanatory Memorandum notes that current Commonwealth criminal law does not contain any offences targeting conduct undertaken by a foreign government that 'falls short of espionage but is intended to harm Australia's national security or influence Australia's political or governmental processes'.[1]

7.5 The Attorney-General's Department submitted that 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.[2]

7.6 Addressing the impact these new foreign interference offences would have on the rights of Australians, the Explanatory Memorandum states:

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

1 Explanatory Memorandum, p. 26.

2 Attorney-General's Department, *Submission 6*, p. 19.

- introducing foreign interference offences, which will criminalise certain conduct that seeks to influence the exercise of Australian democratic or political rights …[3]

7.7 Several participants in the inquiry expressed strong in-principle support for new laws targeting foreign interference in Australia.[4] One participant, for example, submitted:

> It should not be necessary to remind the Australian Government that we as Australian citizens do not wish to see any of our fellow citizens lose their democratic rights and freedoms through interference by a foreign power, and we do not believe that sections of our community should be subjected to subversive or intimidatory pressures.[5]

7.8 Some of these submitters expressed doubts as to whether the new offences in the Bill were broad enough to capture all current foreign interference activity in Australia.[6]

7.9 Some other participants expressed concerns about the potential negative impact of the laws on the rights of Australians. Nyman Gibson Miralis, for example, argued that

> the proposed foreign interference offences significantly, disproportionately and unnecessarily infringe upon various individual rights including the freedom of expression, freedom of religion and even the constitutional guarantee of the implied freedom of political communication.[7]

7.10 The Law Council stated it 'does not support the proposed foreign interference offences in their current form'.[8]

General foreign interference offences

7.11 The general foreign interference offences refer to the offences that appear in Subdivision B (92.2—92.4).

---

3 Explanatory Memorandum, p. 8.

4 Clive Hamilton and Alex Joske, *Submission 20*, p. 2; Federation for a Democratic China, *Submission 32*, p. 3; Professor Rory Medcalf, *Submission 33*, p. 10; Wal Walker, *Submission 42*, pp. [1-2].

5 Wal Walker, *Submission 42*, p. [2].

6 Clive Hamilton and Alex Joske, *Submission 20*, p. 17; Wal Walker, *Submission 42*, pp. [1-2].

7 Nyman Gibson Miralis, *Submission 35*, p. 5.

8 Law Council of Australia, *Submission 5*, p 50.

7.12 The offences in proposed subsections 92.2(1) and 92.3(1) apply where a person engages in conduct on behalf of or in collaboration with a foreign principal (or directed, funded or supervised by a foreign principal), and the person intends that, or is reckless as to whether, their conduct will

- influence a political or governmental process of the Commonwealth or a State or Territory,
- influence the exercise (whether or not in Australia) of an Australian democratic or political right or duty,
- support intelligence activities of a foreign principal, or
- prejudice Australia's national security, and

any part of the conduct

- is covert or deceptive,
- involves the person making a threat to cause serious harm, whether to the person to whom the threat is made or to any other person, or
- involves the person making a demand with menaces.

7.13 The 'targeted person' offences in proposed subsections 92.2(2) and 92.3(2) apply where a person engages in conduct on behalf of or in collaboration with a foreign principal (or directed, funded or supervised by a foreign principal), and the person intends that, or is reckless as to whether, their conduct will influence another person (the *target*)

- in relation to a political or governmental process of the Commonwealth or a State or Territory, or
- in the target's exercise (whether or not in Australia) of an Australian democratic or political right or duty, and

the person 'conceals from, or fails to disclose to, the target their relationship to the foreign principal.

7.14 For the purpose of these offences, the Bill states that the person does not need to have in mind a particular foreign principal and the person may have in mind more than one foreign principal.[9]

7.15 Australian Lawyers for Human Rights noted that the targeted person offences do not require covert, deceptive, threatening or menacing conduct to take place, and could apply to 'kindly and benign' influence if the person

[9] Proposed sections 92.2(3) and 92.3(3).

fails to notify the target of their foreign connection.[10] The group also queried how the targeted person offences would operate in practice:

> One wonders who it is that the perpetrator should be notifying about their attempt to influence a political or government process? What if the target is 'the Australian public'? what if the target is not clear? One also wonders how it is that the perpetrator should notify their target? If the Bill means to say that the perpetrator should make their foreign connection publicly known (even when their 'target' is private), what would achieve this? A statement on a website? A notice in a newspaper? And what does it mean that 'the person does not need to have in mind a particular foreign principal' (as provided in subsection (3) of each proposed section)? How can the perpetrator notify someone that they are acting 'on behalf of' a foreign principal when they do not even have any particular foreign principal in mind?[11]

Meaning of key terms

7.16 The Bill does not define the expression 'political or governmental process of the Commonwealth or a State or Territory'. The Explanatory Memorandum states that that the expression is intended to cover

> matters within political parties (such as which candidate is pre-selected or the manner in which preferences are to be allocated at an election) as well as political matters within the parliamentary process (such as decisions by shadow Cabinet or decisions by political parties about policies).[12]

7.17 The Foreign Influence Transparency Scheme Bill 2017 (FITS Bill) uses a similar expression, namely 'activity for the purpose of political or governmental influence'. Proposed section 12 of the FITS Bill defines this expression as:

- a process in relation to a federal election or a designated vote,
- a process in relation to a federal government decision,
- proceedings of a House of the Parliament,
- a process in relation to a registered political party,
- a process in relation to a member of the Parliament who is not a member of a registered political party,
- a process in relation to a candidate in a federal election who is not endorsed by a registered political party, or

---

10 Australian Lawyers for Human Rights, *Submission 7.1*, p. 3.

11 Australian Lawyers for Human Rights, *Submission 7.1*, p. 3.

12 Explanatory Memorandum, p. 163.

- an activity that influences the public or section of the public in relation to an aspect of any the above processes or proceedings.

7.18 The Attorney-General's Department indicated that the FITS Bill's definition is deliberately limited to federal government processes and that

> [t]he term 'influence a political or governmental process of the Commonwealth or a State or Territory' is not defined, but does explicitly extend to state and territory processes. This provides flexibility for a court to interpret the term based on the admissible evidence.
>
> If the Committee's view is that a definition is desirable, the definition in section 12 of the Foreign Influence Transparency Scheme Bill could provide a useful starting point.[13]

7.19 Similarly, the Bill does not define the expression 'an Australian democratic or political right or duty'. The Explanatory Memorandum states that the expression is intended to

> cover a broad range of rights held by Australians in relation to participation in Australia's democracy, including voting in elections and referenda and participating in lawful protests.[14]

7.20 Australian Lawyers for Human Rights queried whether an 'an Australian democratic or political right or duty' refers to an individual or collective right, and whether the phrase is intended to have a wider meaning than in proposed section 83.4 (the offence of 'interference with political rights and duties'—see Chapter 9).[15]

7.21 The terms 'foreign principal' and 'national security' are defined in proposed sections 90.2 and 90.4 respectively. The breadth of these definitions is discussed in Chapter 3.

Offence for preparing or planning

7.22 Proposed section 92.4 will establish the offence of preparing for, or planning, an offence that appears in Subdivision B (92.2–92.4). The Explanatory Memorandum states:

---

13 Attorney-General's Department, *Submission 6.3*, p. 2.

14 Explanatory Memorandum, p. 92.

15 Australian Lawyers for Human Rights, *Submission 7.1*, p. 23.

> The purpose of this offence is to give law enforcement means to deal with preparatory conduct and enable intervention before foreign interference occurs.[16]

7.23 The Bill structures the offence at proposed section 92.4 similar to the offences for preparing for, or planning, a sabotage and espionage offence, at proposed sections 82.9 and 91.12 respectively.

7.24 General issues concerning the Bill's inclusion of preparatory offences are discussed in Chapter 3.

7.25 The Bill does not define the terms 'planning' and 'preparation'. The Explanatory Memorandum clarifies that these terms are intended to take their ordinary meaning:

- The term 'preparing' could include acts to conceive, formulate, make ready, arrange, and assemble an idea, plan, thing, or person for an offence against another provision in Subdivision A (foreign interference).
- The term 'planning' could include acts to organise, arrange, design, draft, or setup an idea, plan, thing, or person for an offence against another provision in Subdivision A (foreign interference).[17]

7.26 The Law Council contended that

> [t]he preparing for a foreign interference offence in section 92.4 should not proceed. Instead, the ancillary provisions of the Criminal Code for incitement, conspiracy and attempt should be relied upon.[18]

Offences involving foreign intelligence agencies

7.27 Sections 92.7 and 92.8 of the Bill create offences where:

- a person provides support or resources to an organisation or a person acting on behalf of an organisation, and
- the person knows that the organisation is a foreign intelligence agency, or the organisation is a foreign intelligence agency.

7.28 The Explanatory Memorandum states that 'providing support or resources' is intended to cover

---

16 Explanatory Memorandum, p. 180.

17 Explanatory Memorandum, pp. 180-181.

18 Law Council of Australia, *Submission 5*, p. 52.

assistance in the form of providing a benefit or other practical goods and materials, as well as engaging in conduct intended to aid, assist or enhance an organisations activities, operations, or objectives.[19]

Box 7.1 Example—recklessly supporting a foreign intelligence agency

An Australian citizen knows an employee of a foreign government, but does not know the specific agency. The employee insists that the Australian citizen follow specific communication methods whenever in contact, and the Australian is aware that the employee uses several different names.

In response to specific requests, the Australian attends dissident group meetings in Australia and provides a list of attendees to the employee. The Australian also uses open source materials to find identifying details for several of the attendees, which the Australian passes to the employee.[20]

7.29 Sections 92.9 and 92.10 of the Bill create offences where:

- the person directly or indirectly:
  - receives or obtains funds from an organisation,
  - makes funds available to an organisation, or
  - collects funds for or on behalf of an organisation, and
- the person knows that the organisation is a foreign intelligence agency or the organisation is a foreign intelligence agency.

Box 7.2 Example—recklessly funding a foreign intelligence agency

An Australian citizen undertakes ad hoc tasks for foreign individuals employed by a foreign government in return for preferential treatment. Based on the requests made, the Australian suspects these officials are foreign intelligence officers.

In response to a specific request, the Australian attends a prearranged location and gives a large sum of their own money to a foreign individual,

19 Explanatory Memorandum, p. 186.

20 Extrapolated from Explanatory Memorandum, p. 188.

who is visiting and that the Australian has not met before. The Australian does not know what the money will be used for.[21]

7.30 Section 5.6 of the *Criminal Code* applies the 'recklessness' fault element automatically to circumstances, which the Explanatory Memorandum states this requirement:

> [T]he organisation is a foreign intelligence agency and the person was reckless as to this element.[22]

7.31 The Attorney-General's Department noted that the offences in Subdivision C (92.7–92.11) were modelled from the structure of the terrorist organisation offences in sections 102.6 and 102.7 of the *Criminal Code*.[23]

Box 7.3 Existing terrorism offences in the *Criminal Code*

Section 102.6 of the *Criminal Code* outlines the offence for getting funds to, from or for a terrorist organisation. A person commits an offence if:

- the person intentionally:
  - receives funds from, or makes funds available to, an organisation (whether directly or indirectly), or
  - collects funds for, or on behalf of, an organisation (whether directly or indirectly), and
- the organisation is a terrorist organisation, and
- the person knows the organisation is a terrorist organisation, or is reckless as to whether the organisation is a terrorist organisation.

Section 102.7 of the *Criminal Code* outlines the offence for providing support to a terrorist organisation. A person commits the offence if:

- the person intentionally provides to an organisation support or resources that would help the organisation engage in an activity that is directly or indirectly engaged in, preparing, planning, assisting in or fostering the doing of a terrorist act,
- the organisation is a terrorist organisation, and
- the person knows the organisation is a terrorist organisation, or is

21 Extrapolated from Explanatory Memorandum, p. 192.

22 Explanatory Memorandum, p. 188.

23 Attorney-General's Department, *Submission 6.1*, p. 75.

reckless as to whether the organisation is a terrorist organisation.

Both offences are punishable by imprisonment for 25 years or 15 years, depending on whether the person knows the organisation is a terrorist organisation.

Separately, financing terrorism offences exist at sections 103.1 and 103.2 of the *Criminal Code*. These offences require that a person is reckless as to whether the funds will be used to facilitate or engage in a terrorist act and are punishable by life imprisonment.

7.32 The Law Council suggested that the offences in sections 92.7 and 92.8 of the Bill should require that the person intends, or is reckless as to whether, the support or resources would assist a foreign intelligence organisation in an act prejudicial to Australia's security.[24] This suggested change would align the offences closer to existing section 102.7 of the *Criminal Code*.

7.33 Based on the model of the existing financing terrorism offences, namely sections 103.1 and 103.2 of the *Criminal Code*, the Law Council also suggested that sections 92.9 and 92.10

> should require that the person is reckless as to whether the funds will be used to facilitate or engage in activities prejudicial to Australia's national security or, in the case of obtaining funds, involve undue influence.[25]

7.34 The Attorney-General's Department considered that these additional requirements, to align the offences closer to sections 102.7 and 103.1, were not necessary nor appropriate, as the provision of support or funding to a foreign intelligence agency 'in and of itself, presents a threat to Australia's national security'.[26]

7.35 In responding to a question as to why the terrorism offences in section 102.7 explicitly state a fault element of recklessness, while the equivalent offence at proposed section 92.8 does not, the Attorney-General's Department stated:

---

24 Law Council of Australia, *Submission 5*, p. 52.

25 Law Council of Australia, *Submission 5*, p. 52.

26 Attorney-General's Department, *Submission 6.1*, p. 15; Attorney-General's Department, *Submission 6.1*, p. 16.

> The department is not able to clarify why a different approach was taken in the drafting of the existing terrorism offences in section 102.6 and 102.7. However, the effect of both drafting approaches appears to be the same, in that the result is that recklessness is the applicable fault element.[27]

7.36 The joint media organisations expressed concerns about the breadth of the term 'support' in proposed sections 92.7 and 92.8:

> We are concerned that any communication—online, in print or by broadcast—that positively reports about a foreign intelligence agency would breach these sections.[28]

7.37 The organisations brought to the attention of the Committee the case of a Wall Street Journal journalist who was imprisoned in Turkey for engaging in 'terrorist propaganda' through one of her articles.[29] The journalist

> wrote an article about all sides of conflict in a region, including interviewing and reporting the views of the PKK. Because the reporter gave the PKK a voice at all, the article was regarded as terrorist propaganda. Similarly, if any foreign intelligence agency was using a local digital platform and a journalist reported on it, that journalist and the media company would very likely breach the provision.[30]

7.38 The organisations also highlighted an instance in Australia where a news organisation was directed to remove an online article:

> news.com.au wrote a story exposing Islamic State's use of popular online trading sites to target potential victims. News.com.au was directed to remove the story after the Classification Board found that the story indirectly provided instruction on the doing of a terrorism act. The story reported the instructions given to readers of an IS magazine. The Australian Press Council found that the story did not breach the Council's Standards of Practice.[31]

7.39 The joint media organisations recommended that proposed sections 92.7 and 92.8 should become 92.7(1) and 92.8(1) respectively, and should be subject to 92.7(2) and 92.8(2) which should both read:

---

27 Attorney-General's Department, *Submission 6.3*, p. 3.

28 Joint media organisations, *Submission 9*, p. 8.

29 Joint media organisations, *Submission 9*, p. 8; *Submission 9.2*, pp. 6, [9–11].

30 Joint media organisations, *Submission 9*, p. 8.

31 Joint media organisations, *Submission 9.2*, p. 6.

> Publication of information by a journalist in the course of public interest reporting (which may relate to foreign intelligence agencies) does not amount to the provision of 'support' for the purposes of section [92.7(1) /92.8(1)].[32]

7.40 The Attorney-General's Department suggested that the joint media organisations' submission 'reads too much into the word "supports"'. It noted that to commit the offence a person would need to intend to provide support to a foreign intelligence agency.[33]

7.41 At a public hearing, the Attorney-General's Department stated:

> The explanatory memorandum … clarifies that support in that context covers the provision of a benefit or other practical goods or aid. I would also say that that language is consistent with, and mirrors, the language used in the terrorism offences of providing support to a terrorist organisation.[34]

7.42 The Attorney-General's Department also indicated that these offences deliberately do not require the person to intend any outcome, such as harm to Australia's national security.[35]

Defences

7.43 Sections 92.5 and 92.11 of the Bill provide defences to a prosecution to foreign interference offences. The defence applies where the person engaged in conduct that is:

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

7.44 The Explanatory Memorandum states that these defences are appropriate because

> the source of the alleged authority for the defendant's actions is peculiarly within the defendant's knowledge. It is significantly more cost-effective for the

---

32 Joint media organisations, *Submission 9.2*, p. 7.

33 Attorney-General's Department, *Submission 6.1*, p. 34..

34 Ms Anna Harmer, First Assistant Secretary, Attorney-General's Department, *Committee Hansard*, Melbourne, 16 March 2018, p. 36.

35 Attorney-General's Department, *Submission 6.1*, p. 79.

> defendant to assert this matter rather than the prosecution needing to disprove the existence of any authority, from any source.[36]

7.45 The Law Council suggested that the foreign interference offences should provide a defence for persons acting in the public interest.[37] The purpose of the proposed defence would be to protect investigative journalists or ordinary citizens:

> For example, an investigative journalist or a citizen exercising the freedom of expression may engage in 'covert' conduct to influence the exercise of an Australian democratic or political right in collaboration with a person acting on behalf of a foreign principal.[38]

7.46 WWF-Australia also considered that a defence for persons acting in the public interest should be provided for the proposed foreign interference offences.[39]

7.47 The Attorney-General's Department responded:

> It is not clear that conduct constituting a foreign interference offence [can] be excused from criminal liability on the basis that it is 'in the public interest'. Conversely, conduct that [is] 'in the public interest' is unlikely to fall within the scope of the foreign interference offences in the Bill.[40]

7.48 The Law Council argued that a defence for persons acting in their capacity as public officials should not proceed for certain foreign interference offences, namely where:

- a person intends or is reckless as to whether the conduct will prejudice Australia's national security (92.2(1)(c)(iv) and 92.3(1)(c)(iv)),
- any part of the conduct involves the making of threats to cause serious harm (92.2(1)(d)(ii) and 92.3(1)(d)(ii)), and
- any part of the conduct involves making a demand with menaces (92.2(1)(d)(iii) and 92.3(1)(d)(iii)).

7.49 In particular, the Law Council argued:

---

36 Explanatory Memorandum, p. 182.

37 Law Council of Australia, *Submission 5*, p. 52.

38 Law Council of Australia, *Submission 5*, p. 50.

39 WWF-Australia, *Submission 36*, p. 2.

40 Attorney-General's Department, *Submission 6.1*, p. 14.

> Such a defence for public officials appears antithetical to the very intent of the bill—namely, to protect Australia against acts of sabotage, espionage and foreign interference. Furthermore, such a defence would, in practice, be unnecessary in circumstances where a court may consider that the requisite fault elements, once proved by the prosecution, are inconsistent with a public official acting in their capacity.[41]

7.50 The Attorney-General's Department responded that

> There are a range of scenarios in which these defences are appropriate, including where public officials are working with Australia's allies and partners for mutually beneficial outcomes.[42]

Interaction with the Foreign Influence Transparency Scheme Bill 2017

7.51 The Foreign Influence Transparency Scheme Bill 2017 was part of the package of legislative reforms that the Prime Minister introduced on 7 December 2017.[43]

7.52 The Attorney-General's Department indicated that the foreign interference offences and the Foreign Influence Transparency Scheme Bill 2017 are complementary measures and should not be considered in isolation.[44]

7.53 The Law Council outlined its concern about the possible interaction of the proposed foreign interference offences with the Foreign Influence Transparency Scheme Bill 2017:

> If enacted, the Foreign Influence Transparency Scheme Bill 2017 would create criminal offences for intentionally or recklessly not registering under the scheme. Strict liability offences are in place for registrants that fail to notify the Secretary of material changes, report on certain activities, or keep adequate records of activities. A person who is found guilty for one of these strict liability offences may be considered to be operating in a 'deceptive' manner for the purposes of the proposed foreign interference offences.[45]

---

41 Law Council of Australia, *Submission 5*, p. 27.

42 Attorney-General's Department, *Submission 6.1*, p. 7.

43 Attorney-General's Department, *Submission 6*, p. 3.

44 Ms Anna Harmer, First Assistant Secretary, Attorney-General's Department, *Committee Hansard*, Canberra, 31 January 2018, p. 19; Attorney-General's Department, *Submission 6.1*, p. 76.

45 Law Council of Australia, *Submission 5*, p. 51.

7.54 The Law Council called for greater clarity about the interaction between the two Bills in the Explanatory Memorandum:

> [T]he Explanatory Memorandum to the Bill should make clear that a finding of guilt in relation to the Foreign Influence Transparency Scheme Bill 2017 will not necessarily amount to a finding of guilt in relation to the proposed foreign interference offences in the Bill.[46]

7.55 The Attorney-General's Department responded:

> Section 4C of the Crimes Act would prevent a person being prosecuted for both a FITS offence and a foreign interference offence.[47]

7.56 Additionally, the Attorney General's Department stated:

> Registration under the Foreign Influence Transparency Scheme could indicate that a person is engaged in registrable activities for the purpose of influencing a political or governmental process. This may be relevant for paragraphs 92.2(1)(c)) and 92.3(1)(c) …
>
> Registration of activities [under the FITS Bill] will not necessarily mean activities are not covert—noting that a registrant would be unlikely to register in a manner that discloses the commission of an offence.[48]

7.57 Subsection 4C(1) of the *Crimes Act 1914* states that where an act or omission constitutes an offence under two or more laws of the Commonwealth, the offender shall not be liable to be punished twice for the same act or omission.

Consequential amendments

Telecommunications interception

7.58 Under Schedule 4 to the Bill, discussed in Chapter 10, enforcement agencies will be able to apply for a telecommunications interception warrant for the purposes of investigating any of the proposed foreign interference offences.

---

46 Law Council of Australia, *Submission 5*, p. 51.

47 Attorney-General's Department, *Submission 6.1*, p. 16

48 Attorney-General's Department, *Submission 6.1*, pp. 76-77.

Presumption against bail

7.59 Consequential amendments in Schedule 1 to the Bill, discussed in Chapter 10, will impose a presumption against bail for some proposed foreign interference offences.[49] The presumption will apply in circumstances where the defendant is alleged to have made a threat to cause serious harm or a demand with menaces.[50]

Committee comment

7.60 As discussed in Chapter 1, the Committee recognises the need for new laws to respond to the threat of foreign interference in Australia. Unchecked foreign interference has the potential to undermine the integrity of Australia's democracy and threaten the rights and freedoms of Australian people. The Committee therefore supports the introduction of new foreign interference offences.

7.61 However, the Committee notes concerns raised by some participants in the inquiry about the current drafting of the foreign interference offences in proposed Division 92 of the Bill. These included concerns about the definitions of 'foreign intelligence agency' and 'national security' for the purposes of the foreign interference offences. The scope of these terms is discussed in more detail in Chapter 3.

7.62 The Committee notes that section 4C of the Crimes Act deals with situations of 'double jeopardy' and provides that a person cannot be prosecuted twice for the same act or omission. The effect of this provisions is that a person could not be prosecuted under the FITS Bill and a foreign interference offence for the same conduct.

7.63 The Committee notes that the offences in proposed sections 92.7 to 92.10, relating to supporting or funding foreign intelligence agencies, are based on similar existing terrorism offences in sections 102.6 and 102.7 of the *Criminal Code*.

7.64 The Committee notes the Law Council's concerns that, unlike existing terrorism offences, proposed sections 92.7 and 92.8 (knowingly or recklessly supporting foreign intelligence agency) do not include a requirement for recklessness as to whether a person's support would help foreign

---

49 Proposed section 92.2(1) and 92.3(1).

50 *Crimes Act 1914*, proposed section 15AA(2)(e).

intelligence undertake activities that prejudice Australia's national security. However, the Committee notes that the intent of this Bill is to capture behaviour that may not be inherently malicious, but may nonetheless assist foreign intelligence agencies—for example, facilitating travel arrangements within Australia to enable covert activities. Consequently, the Committee considers that including this further requirement is not appropriate and may reduce the effectiveness of the provisions.

7.65 The Committee has considered concerns expressed by the joint media organisations that the term 'support' in proposed sections 92.7 and 92.8 could extend to journalists reporting positively, or neutrally, about a foreign intelligence agency. The Committee notes the intention expressed in the Explanatory Memorandum that the term 'support' covers the provision of a benefit or other practical goods or aid, and therefore would be unlikely to apply to the examples provided by the media organisations. However, the Committee considers that further clarity would be achieved through amending the Bill to make explicit that the term 'support' refers to 'material support' and providing examples in the Explanatory Memorandum.

Recommendation 42

7.66 The Committee recommends that the Bill be amended to explicitly provide that the term 'support' refers to 'material support', and that the Explanatory Memorandum provide examples of conduct that will not constitute material support, for example, news reporting, editorial or opinion writing and humanitarian assistance.

7.67 In relation to proposed sections 92.9 and 92.10 (Knowingly, or recklessly, funding or, being funded by foreign intelligence agency) the Committee considers that the financing terrorism offences in sections 103.1 and 103.2 of the *Criminal Code* are not an appropriate comparison for these offences. Rather, the offences are based on existing section 102.6 (Getting funds to, from or for a terrorist organisation). In comparing the proposed new offences with section 102.6, the Committee is satisfied that no additional elements are required in sections 92.9 and 92.10.

7.68 The Committee notes the intent of the Bill to include preparatory offences targeting activities that may fall short of 'attempt' under section 11.1 of the *Criminal Code*. The Bill's use of preparatory offences was discussed in general terms in Chapter 3. The Committee considers that the ability to prosecute and prevent foreign interference is a key function of the Bill and

therefore considers that the preparing and planning offences for foreign interference should remain.

Theft of trade secrets

7.69 Schedule 1 will also amend Part 5.2 of the *Criminal Code* to insert a new offence for theft of trade secrets involving a foreign government principal (Division 92A).

7.70 The new offence and proposed penalty is set out below.

Table 7.2 Theft of trade secrets involving foreign government principal

Offence	Section	Penalty	Aggravated offences
Theft of trade secrets involving foreign government principal	92A(1)	15 years	Nil

Overview of the offence

7.71 Proposed Division 92A is intended to protect 'trade secrets' by making it an offence to dishonestly receive, obtain, take, copy or duplicate, sell, buy or disclose certain information where the conduct is connected to a foreign government principal.

7.72 In contrast to a number of other offences in Part 5.2 of the *Criminal Code*, the proposed offence of theft of trade secrets does not contain a 'national security' element. The offence arises where:

- a person intentionally and dishonestly receives, obtains, takes, copies or duplicates, sells, buys or discloses information; and
- all of the following circumstances exist, and the person is reckless as to these circumstances:
  - the information was not generally known in trade or business, or in that particular trade or business concerned,
  - the information has a commercial value that would be, or could reasonably be expected to be, destroyed or diminished if the information were communicated, and
  - the owner of the information had made reasonable efforts in the circumstances to prevent that information from becoming generally known, and

- any of the following circumstances apply, and the person is reckless as to this element:
  - the person engaged in the conduct on behalf of a foreign principal,
  - the person engaged in the conduct on behalf of a person acting on behalf of a foreign principal,
  - the person engaged in the conduct in collaboration with a foreign principal,
  - the person engaged in the conduct in collaboration with a person acting on behalf of a foreign principal,
  - the conduct was directed, funded or supervised by a foreign principal, or
  - the conduct was directed, funded or supervised by a person acting on behalf of a foreign principal.

7.73 The person does not need to have in mind a particular foreign government principal, and may have more than one foreign government principal in mind.

7.74 Although the term 'trade secret' is not used in the wording of the offence, the Explanatory Memorandum provides that it is intended that the offence will protect this type of information, consistent with comparative international laws.[51] The Explanatory Memorandum characterises the theft of trade secrets as 'economic espionage'.[52]

7.75 The proposed sabotage, espionage and foreign interference offences arise in connection to a 'foreign principal'. In contrast, the offence in proposed section 92A arises in connection to the more narrowly defined concept of a 'foreign government principal'. Proposed section 90.3 of the Bill defines 'foreign government principal' as:

- a foreign country's government or the government of part of a foreign country,
- an authority of the foreign country's government, or an authority of part of a foreign country,
- a local or regional government body of a foreign country,
- a foreign public enterprise,[53]

---

51 Explanatory Memorandum, p. 200 .

52 Explanatory Memorandum, p. 3.

53 Proposed section 90.3(e) and (f) provide that the term 'foreign government principal' includes a company to which any of the subparagraphs of paragraph (a) of the definition of foreign public enterprise in section 70.1 of the *Criminal Code* applies; and a body or association to which either

- a foreign political organisation, and
- entities or organisations owned, directed or controlled by a foreign government principal or multiple foreign principals from the same foreign country.

7.76 The Bill defines 'dishonest' to mean:

> … dishonest according to the standards of ordinary people; and known by the defendant to be dishonest according to the standards of ordinary people.[54]

7.77 The Bill proposes to apply a modified form of extended geographical jurisdiction 'Category B' to the theft of trade secrets. An offence will be within jurisdiction if:

- the conduct constituting the offence occurs wholly or partly in Australia
- the result of that conduct occurs wholly or partly in Australia, and
- the conduct occurs outside Australia and at the time of committing the offence, the person is an Australian citizen, resident or body corporate;[55]

but

- the defendant will not be able to avoid prosecution on the basis that the country in which he or she committed the offence does not have a corresponding economic espionage/theft of trade secrets offence.[56]

7.78 The Bill also proposes enabling law enforcement agencies to obtain a telecommunications interception warrant to investigate this offence.[57]

Rationale for the new offence

7.79 In its submission, the Attorney-General's Department outlined that the purpose of the new offence is

---

of the subparagraphs of paragraph (b) of the definition of foreign public enterprise applies. The effect of these paragraphs is that all foreign public enterprises are included.

54 Proposed section 92A.1(2).

55 *Criminal Code*, section 15.2.

56 Proposed section 92A.2(1) applies section 15.2 (extended geographical jurisdiction—Category B) to section 92A.1, but provides that subsections 15.2(2) and 15.2(4) of the section do not apply. Refer also to Explanatory Memorandum, p. 202.

57 Schedule 4 of the Bill will amend the definition of 'serious offence' in s. 5D(1)(e) of the *Telecommunications (Interception and Access) Act 1979*.

> to combat the increasing threat of data theft, business interruption and economic espionage, particularly by or on behalf of foreign individuals and entities.[58]

7.80 The Department referred to ASIO's 2016–2017 Annual Report, which stated:

> 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.[59]

7.81 The Department noted that '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'.[60] Its submission identified potential targets of economic espionage as including

> 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).[61]

7.82 The Department noted that Australia 'lags behind' the comparable jurisdictions of New Zealand, Canada and the United States in relation to having specific offences for economic espionage.[62] The Department drew the Committee's attention to a number of convictions under the United States offence, with examples including theft of microchip blueprints, secrets related to military training, aviation technology information and wireless technology.[63]

7.83 Conversely, the Law Council of Australia noted that the United Kingdom does not criminalise economic espionage.[64]

---

58 Attorney-General's Department, *Submission 6*, p. 18.

59 Attorney-General's Department, *Submission 6*, p. 6; citing Australian Security Intelligence Organisation, *Annual Report 2016-2017*, p. 23.

60 Attorney-General's Department, *Submission 6*, p. 18.

61 Attorney-General's Department, *Submission 6*, p. 18.

62 Attorney-General's Department, *Submission 6*, p. 7.

63 Attorney-General's Department, *Submission 6*, p. 56; Ms Tara Inverarity, Assistant Secretary, Attorney-General's Department, *Committee Hansard*, Canberra, 31 January 2018, p. 21.

64 Law Council of Australia, *Submission 5*, p. 53.

7.84 The Director-General of Security outlined at a public hearing the threat posed by foreign intelligence services to private sector interests:

> Foreign spies are now not only interested in government information; we know that they also pursue privileged information and intellectual property from the private sector. That includes the agricultural sector, the mining technology field, medical research, the tertiary institution research and development field and, of course, the financial sector data.[65]

7.85 ASIO noted that there have been instances of Australian companies facing significant financial loses as a result of this type of activity:

> We have examples of where, both through cyber and human means, foreign intelligence services have targeted major resource companies, our financial institutions et cetera, with a view to obtaining information from those particular organisations. … We know of instances where Australian companies, for instance, have lost hundreds of millions of dollars through the stealing of intellectual property, et cetera, et cetera, where that information has been taken—stolen—as I said, by human and cyber means and taken back to the particular country in question and used for their own purposes.[66]

7.86 Mr Peter Jennings noted that a number of states have increased efforts to steal intellectual property.[67] Mr Jennings submitted that the introduction of laws aimed at countering the theft of trade secrets was 'timely and necessary'.[68]

7.87 Professor Rory Medcalf commented that intelligence secrets and intellectual property, including scientific research, obtained from Australia could be used by foreign powers to attain a military and economic edge:

> Some of this information is held by the Australian Government and the Australian Defence Force; some is held within private companies; and some is potentially embodied within academic research.[69]

---

65 Mr Duncan Lewis, Director-General of Security, Australian Security Intelligence Organisation, *Committee Hansard*, Melbourne, 16 March 2018, p. 34.

66 Mr Peter Vickery, Deputy Director-General, Counter-Espionage and Interference and Capabilities, Australian Security Intelligence Organisations, *Committee Hansard*, Canberra, 31 January 2018, p. 21.

67 Peter Jennings, *Submission 15*, p. 1.

68 Peter Jennings, *Submission 15*, p. 1.

69 Rory Medcalf, *Submission 33*, p. 3.

Penalty

7.88 The offence will be punishable by a maximum penalty of 15 years imprisonment. The Explanatory Memorandum provides:

> The commission of this offence would have serious consequences for Australia's security and economic interests. It is unacceptable for foreign principals to seek to interfere in Australia's commercial dealings and trade relations. The penalty is consistent with comparable offences in which provide for a link with a foreign principal including section 91.8 (espionage on behalf of a foreign principal) and section 92.3 (offence of reckless foreign interference).[70]

Defences

7.89 The general defences set out in Part 2.3 of the *Criminal Code* will be available. The Bill does not propose offence-specific defences.

Attorney-General's Consent

7.90 Consistent with other Part 5.2 offences, the consent of the Attorney-General will be required before a person can be committed for trial.[71] The Attorney-General's consent is not required to arrest, charge or remand an accused person in custody or on bail.

7.91 Human Rights Watch submitted that the consent requirement is not sufficient to remedy the threat to liberty that the trade secret offence carries.[72]

Civil versus criminal enforcement

7.92 The Law Council of Australia did not support the proposed offence, arguing that persons and organisations affected by economic espionage should pursue civil enforcement. In support of its recommendation that the offence does not proceed, the Law Council noted a number of difficulties in criminalising theft of trade secrets, including that:

- the public would bear the cost of these prosecutions;
- there is a lack of evidence that criminal sanctions would have a greater deterrent effect than civil law; and

---

70 Explanatory Memorandum, p. 202.

71 Proposed section 93.1.

72 Human Rights Watch, *Submission 10*, p. 5.

- criminal sanctions may draw greater publicity, which could deter victims from coming forward.[73]

7.93 In response, the Attorney-General's Department distinguished between the theft of trade secrets on behalf of a foreign government, and theft of trade secrets conducted by other actors. The Attorney-General's Department submitted that the former 'amounts to economic espionage which is harmful to Australia's national security and economic prosperity' and is thus criminalised. The Bill does not propose to criminalise the latter, recognising that '[t]his is properly left to civil enforcement mechanisms or state/territory theft offences'.[74]

7.94 The Director-General of Security spoke of malicious foreign actors taking advantage of a number of 'gaps' in Australian laws. In relation to the proposed secrecy, espionage, sabotage and trade secrets offences, the Director-General advised:

> I believe these new laws are needed urgently. There's a pressing requirement to deter hostile foreign spies who are conducting espionage and foreign interference against Australian interests as we sit here today. The proposed laws would, in my view, make Australia a much harder target for foreign intelligence services.[75]

7.95 Describing the current environment, the Director-General commented:

> [F]acing no realistic prospect of criminal investigation and prosecution for their activities against us, our foreign adversaries are currently shielded from the significant disincentive of public exposure and punishment, and they are taking advantage of this gap. … Criminal prosecutions for espionage, foreign interference, secrecy, sabotage and economic espionage offences that are tested in our courts and reported in our media will send a very powerful message to those orchestrating such activity against us. Prosecutions will also discourage individuals from being caught up in these activities.[76]

---

73 Law Council of Australia, *Submission 5,* p. 53.

74 Attorney-General's Department, *Submission 6.1,* p. 16.

75 Mr Duncan Lewis, Director-General of Security, Australian Security Intelligence Organisation, *Committee Hansard*, Melbourne, 16 March 2018, p. 34.

76 Mr Duncan Lewis, Director-General of Security, Australian Security Intelligence Organisation, *Committee Hansard*, Melbourne, 16 March 2018, p. 34.

7.96 The Law Council also raised concerns that criminal sanctions would not compensate the owners of trade secrets for their loss.[77] The Department responded:

> In terms of compensation, section 21B of the *Crimes Act* allows a sentencing court to make an order requiring an offender to make reparation to any person, by way of money payment or otherwise, in respect of any loss suffered, or any expense incurred, by the person by reason of the offence.[78]

Committee Comment

7.97 Throughout this inquiry, the Committee has reviewed offences with a view to ensuring that each offence is sufficiently clear and unambiguous; enforceable; and appropriately targeted and proportionate to the threat. For most offences the threat has been to our national security. In the case of the theft of trade secrets offence, it is worth noting that the direct threat is to private interests – that is, the offence endeavours to protect private interests from threats to their proprietary information.

7.98 The Committee notes the concerns raised by the Law Council of Australia that, as the proposed new offence protects private interests, it would be more appropriately pursued privately by the affected person (that is, under the civil law).

7.99 However the Committee notes the rationale expressed in the Explanatory Memorandum that the theft of trade secrets on behalf of a foreign government amounts to economic espionage, and that this conduct 'can severely damage Australia's national security and economic interests'.[79] The Committee also notes the advice provided by ASIO about the range of private sector interests that have been targeted by foreign government actors in the past,[80] and the substantial economic losses incurred by Australian companies as a result.[81]

---

77 Law Council of Australia, *Submission 5,* p. 53.

78 Attorney-General's Department, *Submission 6.1,* p. 86.

79 Explanatory Memorandum, p. 27.

80 Mr Duncan Lewis, Director-General of Security, Australian Security Intelligence Organisation, *Committee Hansard*, Melbourne, 16 March 2018, p. 34.

81 Mr Peter Vickery, Deputy Director-General, Counter-Espionage and Interference and Capabilities, Australian Security Intelligence Organisations, *Committee Hansard*, Canberra, 31 January 2018, p. 21.

7.100 The Committee recognises that non-government bodies and other private citizens hold information that could, if acquired by a foreign government actor, be used to disadvantage Australia's national security. Further, the coordinated theft of trade secrets by foreign government actors could, in the long term, substantially diminish Australia's economic wellbeing and competitiveness. Accordingly, the Committee accepts the necessity of the provisions to deter privately held 'trade secrets' from being targeted by foreign state actors, and to provide law enforcement and prosecutors with the tools they need to respond to this type of theft.

7.101 In relation to the detail of the provisions, the Committee questions whether it is sufficiently clear that the proposed threshold of 'dishonestly' stealing trade secrets would capture economic espionage committed by cyber vectors—for example, by hacking into a company's electronic records in order to access commercially sensitive information and intellectual property. The Committee recommends that, if this conduct is intended to be captured by the offence, then this should be reflected in the Explanatory Memorandum.

Recommendation 43

7.102 The Committee recommends that the Explanatory Memorandum be amended to clarify whether the offence is intended to capture the theft of trade secrets by hacking or other online vectors.

8. Sabotage offences

8.1 This chapter discusses the Bill's proposed new offences relating to sabotage.

8.2 The Bill replaces the two current sabotage offences in the *Crimes Act 1914* (Crimes Act) with seven new offences in the *Criminal Code* (Division 82). While the existing offences are limited to defence property,[1] the proposed new sabotage offences are premised on damage or vulnerabilities to 'public infrastructure'.

8.3 The seven new offences, the relevant section and proposed penalties are set out below.

Table 8.1 Sabotage Offences

Offence	Section	Penalty
Sabotage – involving foreign principal with intention as to national security	82.3	25 years
Sabotage – involving foreign principal reckless as to national security	82.4	20 years
Sabotage – with intention as to national security	82.5	20 years
Sabotage – reckless as to national security	82.6	15 years
Introducing vulnerability – with intention as to national security	82.7	15 years
Introducing vulnerability – reckless as to national security	82.8	10 years

[1] See *Crimes Act 1914*, s. 24AB.

Preparing for or planning sabotage	82.9	7 years

8.4 The Department explained the intention behind the broadening of the sabotage offences beyond conduct against defence property:

> [T]he broadening of the sabotage offences is really to recognise the importance of protecting Australia's critical infrastructure and our heavy reliance on that infrastructure to maintain a prosperous society. Effectively, the existing offence that protects only defence facilities recognises a time when defence was of peak interest, but really we rely on a much broader range of infrastructure. The offences will criminalise the acts of interfering with a broader range of critical infrastructure—of acting to directly sabotage that infrastructure. It's intended to act as a deterrent but also to provide a mechanism for prosecution where there are acts to sabotage or introduce vulnerabilities into Australia's critical infrastructure.[2]

8.5 The general requirements for the offences in sections 82.3 to 82.6 are that a person engages in conduct and the conduct results in 'damage to public infrastructure'; and the person intends that, or is reckless as to whether, the conduct will

- prejudice Australia's national security, or
- advantage the national security of a foreign country.

8.6 The offences in 82.3 and 82.4 also require that any of the following circumstances exists:

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

Definitions of 'damage to public infrastructure' and 'public infrastructure'

8.7 Underpinning the new sabotage offences are the definitions of 'damage to public infrastructure' and 'public infrastructure'.

---

[2] Ms Anna Harmer, First Assistant Secretary, Security and Criminal Law Division, Attorney-General's Department, *Committee Hansard*, Canberra, 31 January 2018, p. 22.

8.8 Proposed section 82.1 of the *Criminal Code* provides that conduct results in damage to public infrastructure if any of the following applies in relation to public infrastructure:

a. the conduct destroys it or results in its destruction,

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

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

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

e. the conduct results in it or any part of it becoming defective or being contaminated,

f. the conduct significantly degrades its quality,

g. if it is an electronic system—the conduct seriously disrupts it.[3]

8.9 Noting in particular paragraph (d) of this definition, the Committee enquired as to whether otherwise lawful dissent and protest could be captured under the sabotage offences (for example, protest action, such as blockades, sit-ins or pickets, that is specifically designed to limit people's access to their places or work). The Attorney-General's Department responded:

> The sabotage offences only apply where a person intended to prejudice Australia's national security or advantage the national security of a foreign country (or, in relation to sections 82.7 and 82.8, to harm or prejudice Australia's economic interests, disrupt the functions of government or damage public infrastructure). The burden will be on the prosecution to prove these elements beyond a reasonable doubt.[4]

8.10 'Public infrastructure' is broadly defined in section 82.2(1) as follows:

a. any infrastructure, facility, premises, network or electronic system that belongs to the Commonwealth;

b. defence premises within the meaning of Part VIA of the 24 *Defence Act 1903*;

---

3 Proposed section 82.1.

4 Attorney-General's Department, *Submission 6.1*, p. 81.

c. service property, and service land, within the meaning of the *Defence Force Discipline Act 1982*;

d. any part of the infrastructure of a telecommunications network within the meaning of the *Telecommunications Act 1997*;

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

i. provides or relates to providing the public with utilities or services (including transport of people or goods) of any kind; and

ii. is located in Australia; and

iii. belongs to or is operated by a constitutional corporation or is used to facilitate constitutional trade and commerce.[5]

8.11 The Explanatory Memorandum explains the importance of the definition of public infrastructure as follows:

> The definition of public infrastructure covers infrastructure and services that are essential to everyday life in Australia. A disruption to public infrastructure due to sabotage could have a range of serious implications for business, governments and the community.[6]

8.12 The proposed definition includes telecommunications networks and other networks and electronic systems (see paragraphs a, d, and e). The Attorney-General's Department confirmed that, for the purpose of the offences in proposed sections 82.7 and 82.8 (introducing vulnerability), individual mobile phones, laptops and tablets would fall within the scope of 'articles' and/or 'things' that may be part of public infrastructure.[7]

8.13 For the purpose of subparagraph (e)(i) of the definition, 'constitution corporation' means a corporation to which paragraph 51(xx) of the Constitution applies.[8] This would include most businesses that have 'Pty Ltd' or 'Ltd' within its business name, and other entities considered to be

---

5 Proposed section 82.2.

6 Explanatory Memorandum, p. 40.

7 Attorney-General's Department, *Submission 6.1*, p. 82.

8 *Criminal Code*, Dictionary. Paragraph 51(xx) of the Constitution provides that the Parliament has power to make laws for the peace, order and good government of the Commonwealth with respect to 'foreign corporations, and trading or financial corporations formed within the limits of the Commonwealth'.

'trading corporations'.[9] 'Constitutional trade and commerce' is defined in the Bill to mean trade and commerce with other countries, among the States, between a State and a Territory, or between two Territories.[10]

8.14 The Explanatory Memorandum provides the following explanation as to why the definition of 'public infrastructure' also includes privately-owned infrastructure:

> It is essential to cover privately owned infrastructure within the definition of public infrastructure because the consequences flowing from damage to these types of infrastructure could be as damaging as damage to infrastructure owned by the Commonwealth.[11]

8.15 The joint councils for civil liberties considered that the combination of the definition of public infrastructure and that of damage to public infrastructure

> … could capture conduct of minor significance in terms of actual harm done to the infrastructure or harm to infrastructure that has no significant relationship with an appropriately defined 'national security'.[12]

Critical infrastructure versus public infrastructure

8.16 The Explanatory Memorandum states that the Bill 'introduces comprehensive new sabotage offences that effectively protect *critical infrastructure* in the modern environment'.[13]

8.17 Whilst the Explanatory Memorandum refers to critical infrastructure, the Bill refers to 'public infrastructure'. This is a broader term than critical infrastructure as defined in the Security of Critical Infrastructure Bill 2017 (recently reviewed by this Committee) which defines critical infrastructure as:

---

9 See Fair Work Ombudsman, 'Dictionary': < https://www.fairwork.gov.au/Dictionary.aspx?FirstLetter=c> viewed 9 March 2018. Non-constitutional corporations include sole traders, partnerships, trusts, certain state government public sector employers, and corporations whose main activity is not trading or financial. See Fair Work Commission, 'Coverage': <https://www.fwc.gov.au/about-us/the-national-workplace-relations-system/coverage> viewed 9 March 2018.

10 Schedule 1, item 24.

11 Explanatory Memorandum, p. 43.

12 Joint councils for civil liberties, *Submission 31*, p. 46

13 Explanatory Memorandum, p. 2 (emphasis added).

- a critical electricity asset; or
- a critical port; or
- a critical water asset; or
- a critical gas asset; or
- an asset declared under section 51 to be a critical infrastructure asset; or
- an asset prescribed by the rules.[14]

8.18 The Committee raised this discrepancy with the Attorney-General's Department, which stated that:

> The Explanatory Memorandum uses the term 'critical infrastructure' because this is a commonly used and understood term in public discourse. The term 'public infrastructure' was adopted in the Bill as the best technical description for the matters covered by the definition. This was a drafting matter.[15]

8.19 The Committee also asked the Department why the Bill is not constrained to critical infrastructure as defined in the Security of Critical Infrastructure Bill 2017. The Department stated:

> The purpose of the Bills is quite different and it is not necessary for the definitions to completely align. The harm that comes from damage to public infrastructure due to sabotage is deserving of criminalisation on its own merits.
>
> The Security of Critical Infrastructure Bill is targeted at specific assets and sectors where the risk from espionage, sabotage and coercion is highest. It is designed to ensure that Government has all the necessary information to conduct risk assessments and the powers to enforce mitigations if they are not implemented through collaboration. Given it is imposing a regulatory burden, it is drafted with a narrower focus.[16]

Intention and recklessness as to national security

8.20 The offences in proposed sections 82.3 and 82.5 require that a person *intends* to

- prejudice Australia's national security; or
- advantage the national security of a foreign country.

---

14 Security of Critical Infrastructure Bill 2017, proposed section 9.

15 Attorney-General's Department, *Submission 6.1*, p. 84.

16 Attorney-General's Department, *Submission 6.1*, p. 84.

8.21 The offences in proposed sections 82.4 and 82.6, however, only require that a person is *reckless* to these elements.

8.22 Similarly, the offences in proposed sections 8.28 and 82.8 (introducing vulnerability offences) require a person to intend, or be reckless as to whether the following will occur:

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

8.23 Proposed section 90.4 defines the term 'national security' to include a country's political, military or economic relations with another country or other countries. The breadth of this term, and the meaning of the words 'prejudice' and 'advantage', is discussed in detail in Chapter 3.

8.24 As also discussed in Chapter 3, section 5.4 of the *Criminal Code* provides that a person is reckless with respect to:

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

8.25 The Committee noted that private contractors or Commonwealth officials may be aware of substantial risks when carrying out work, such as repairs, to critical infrastructure (or, in the case of information and communications technology, when carrying out updates and upgrades to a network) but be required to carry out that work anyway. The Committee asked the Attorney-General's Department whether a person carrying out dangerous and difficult repairs to a large piece of infrastructure could be considered to be reckless. The Department responded:

> In the context of essential repairs to public infrastructure, the risk is likely to be justified.

> The elements of the sabotage offences also require a person to have intended to, or be reckless as to whether his or her conduct would, prejudice Australia's national security or advantage the national security of a foreign country.[17]

Harm or prejudice to Australia's economic interests, and other matters

8.26 Proposed sections 82.7 and 82.8 establish new offences for introducing a vulnerability with the intention that the following will occur:

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

8.27 The Explanatory Memorandum explains that the term 'prejudice',

> … is intended to capture a broad range of intended conduct, including an intention to harm or injure Australia's national security or to cause disadvantage to Australia. The term is also intended to cover impairment or loss to Australia's national security interests. The prejudice to Australia's national security is not required to be serious or substantial but is intended to be more than a minor or trivial prejudice that has no long-lasting effect, nor embarrassment to an Australian person or Australia's people.[18]

8.28 The Law Council of Australia was concerned that the intention expressed in the Explanatory Memorandum is not borne out in the text of the Bill, namely that prejudice is not required to be serious or substantial but is intended to be more than a minor or trivial prejudice.[19]

8.29 Unlike other sabotage offences, proposed sections 82.7 and 82.8 do not necessarily require the person to intend or be reckless as to whether their conduct will prejudice Australia's national security, or advantage another country's national security. The offence could be made out if the person intended or was reckless as to whether their conduct will:

---

17 Attorney-General's Department, *Submission 6.1*, pp. 79–80.

18 Explanatory Memorandum, p. 68.

19 Law Council of Australia, *Submission 5*, p. 34.

- harm or prejudice Australia's economic interests,[20]
- disrupt government functions,[21] or
- damage public infrastructure.[22]

8.30 The Committee asked the Department if the drafting of the offence in a way that takes it outside of the national security context was deliberate. The Department provided the following answer:

> The sabotage offences in sections 82.7 and section 82.8 will apply if a person engages in the conduct with the intention to prejudice Australia's national security (subparagraph 82.7(d)(i)) or is reckless as to whether his or her conduct would prejudice Australia's national security (subparagraph 82.8(d)(i)). They will also apply in the circumstances listed [in the above paragraph].[23]

8.31 When asked why the additional element of 'harm or prejudice to Australia's economic interests' was included for the introducing vulnerability offences, the Department responded:

> The sabotage offences in sections 82.3 to 82.6 require a person to have actually damaged public infrastructure. The prosecution will have proved that the person was reckless as to this element when proving the damage to public infrastructure. Therefore, it is not necessary to also prove that the person intended to disrupt government services or harm Australia's economic interests.
>
> This is not the case with the offences in sections 82.7 and 82.8 where damage has not necessarily yet occurred, but a vulnerability has been created. Therefore, these offences have a broader range of matters listed in relation to the person's intention at the point that he or she introduced the vulnerability.[24]

Preparing for or planning a sabotage offence

8.32 Proposed section 82.9 provides that person commits an offence if they engage in conduct with the intention of preparing for, or planning, an

---

20 Proposed sections 82.7(d)(ii) and s. 82.8(d)(ii).

21 Proposed sections 82.7(d)(iii) and s. 82.8(d)(iii).

22 Proposed sections 82.7(d)(iv) and s. 82.8(d)(iv).

23 Attorney-General's Department, *Submission 6.2*, pp. 5–6.

24 Attorney-General's Department, *Submission 6.1*, p. 83.

offence against Division 82. Separately, Part 2.4 of the *Criminal Code* already contains incitement, conspiracy and attempt provisions.

8.33 General issues concerning the Bill's inclusion of preparatory offences are discussed in Chapter 3.

8.34 The Law Council of Australia raised the following specific concern about the preparatory sabotage offence:

> [T]he extension of criminal responsibility to cover preparatory acts requires law enforcement and prosecutorial authorities to exercise a considerable degree of discretion when determining whether an otherwise innocuous act should be subject to the charge and prosecution. In the Law Council's view, an unacceptable element of arbitrariness and unpredictability may arise in determining whether or not a person is charged with the preparatory offence under proposed section 82.9.[25]

Penalties

8.35 The existing penalty for sabotage is imprisonment for 15 years whilst the penalties proposed for the expanded sabotage offences are as high as 25 years imprisonment.

8.36 Sections 82.7 and 82.8 establish offences which include introducing vulnerability with the intention to harm or prejudice to Australia's economic interests. That prejudice is 'not required to be serious or substantial'. The Committee sought clarification from the Attorney-General's Department as to whether such conduct is proportionate to the proposed penalties of ten to 15 years imprisonment. The Department answered that:

> Consistent with Commonwealth criminal law policy, the maximum penalty for an offence should be set appropriately for the worst case scenario.[26]

8.37 Additionally, the Department pointed to the Explanatory Memorandum's justification for the penalty for the offence at section 82.7 (offence of introducing vulnerability with intention as to national security):

> The offence will be punishable by a maximum penalty of 15 years imprisonment. The commission of this offence would have serious consequences for Australia's national security and economic interests. It is

---

25 Law Council of Australia, *Submission 5*, p. 35.

26 Attorney-General's Department, *Submission 6.1*, p. 9.

> unacceptable for persons to enable the misuse, impairment or unauthorised access or modification of an article, thing or software that is or is part of public infrastructure. In the worst case scenario, Australians could be killed or seriously harmed as a result of the modification or impairment of public infrastructure by a person intending to harm Australia's national security. This justifies the serious maximum penalty for the offence.[27]

8.38 With respect to the penalty for the offence at section 82.8 (offence of introducing vulnerability reckless as to national security), the Explanatory Memorandum reasoned:

> The offence will be punishable by a maximum penalty of 10 years imprisonment. The commission of this offence would have serious consequences for Australia's national security and economic interests. It is unacceptable for persons to enable the misuse, impairment or unauthorised access or modification of an article, thing or software that is or is part of public infrastructure. In the worst case scenario, Australians could be killed or seriously harmed as a result of the modification or impairment of public infrastructure by a person who is reckless as to the harm that may result. This justifies the serious maximum penalty for the offence.[28]

Defences

8.39 Section 82.10 of the Bill provides a defence for conduct where a person is engaged in accessing or using a computer or other electronic system and the person engaged in the conduct in the person's capacity as a public official. The Law Council's submission noted that this defence is 'far more limited than the current defence which applies to acts done in good faith'.[29]

8.40 In addition, the Law Council submitted that a defence for where the person engaged in conduct in the person's capacity as a public official should not be available for sabotage offences:

> The Law Council considers that a person acting in their capacity as a public official should not be permitted to act with the intention of, or be reckless as to, prejudicing Australia's national security. Such a defence for public officials appears antithetical to the very intent of the Bill, namely, to protect Australia against acts of sabotage, espionage and foreign interference. Furthermore, such a defence would in practice be unnecessary in circumstances where a

---

27 Explanatory Memorandum, p. 64.

28 Explanatory Memorandum, p. 69.

29 Law Council of Australia, *Submission 5*, p. 36.

> court may consider that the requisite fault elements once proven by the prosecution are inconsistent with a public official acting in their capacity.[30]

8.41 The Law Council gave a specific example to demonstrate its position that the defence is unnecessary:

> Proposed section 82.3 would provide an offence for where a person engages in conduct resulting in damage to public infrastructure intending that the conduct will prejudice Australia's national security. The conduct must be engaged in on behalf of, or in collaboration with, a foreign principal or a person acting on behalf of a foreign principal. Alternatively, the conduct must be directed, funded or supervised by a foreign principal or a person acting on behalf of a foreign principal. Proposed section 82.10 would provide a defence for a person who accessed or used a computer or other electronic system and they engaged in the conduct in their capacity as a public official. However, the Law Council submits that a person acting in their capacity as a public official would not intend to prejudice Australia's national security. The defence is unnecessary.[31]

8.42 In response, the Department stated that 'there are a range of scenarios in which these defences are appropriate, including where public officials are working with Australia's allies and partners for mutually beneficial outcomes'.[32]

8.43 The Committee asked the Department, given that the Bill's definition of 'public infrastructure' extends to infrastructure that is privately operated, whether there should be a defence available for conduct undertaken on behalf of the private company (in addition to conduct in a person's capacity as a public official). The Department agreed that the existing defence 'could be broadened to cover conduct undertaken on behalf of a private owner'.[33]

8.44 Under the existing 'good faith' defence in section 24F of the Crimes Act, it is a defence to a charge of treachery or sabotage if a person has:

> (a) endeavoured in good faith to show that the Sovereign, the Governor-General, the Governor of a State, the Administrator of a Territory, or the

---

30 Law Council of Australia, *Submission 5*, p. 26. The Law Council extended this point to espionage and foreign interference offences.

31 Law Council of Australia, *Submission 5*, p. 27.

32 Attorney-General's Department, *Submission 6.1*, p. 6.

33 Attorney-General's Department, *Submission 6.1*, p. 80.

advisers of any of them, or the persons responsible for the government of another country, has or have been, or is or are, mistaken in any of his, her or their counsels, policies or actions;

(b) pointed out in good faith errors or defects in the government, the constitution, the legislation or the administration of justice of or in the Commonwealth, a State, a Territory or another country, with a view to the reformation of those errors or defects;

(c) excited in good faith another person to attempt to procure by lawful means the alteration of any matter established by law in the Commonwealth, a State, a Territory or another country;

(d) pointed out in good faith, in order to bring about their removal, any matters that are producing, or have a tendency to produce, feelings of ill-will or hostility between different classes of persons; or

(e) done anything in good faith in connexion with an industrial dispute or an industrial matter.

8.45 Subsection 24F(2) of the Crimes Act then outlines several situations where it cannot be said that an act or thing is done in good faith.

8.46 The Law Council submitted that:

> The physical elements of the sabotage offences are broad and an important safeguard in relation to these offences is the availability of adequate defences. The Law Council considers that there should be a good faith defence appropriately adapted to the new sabotage offences in the absence of sufficient justification to the contrary.[34]

8.47 The Department advised that a good faith defence was 'not considered appropriate' and stated that:

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

[34] Law Council of Australia, *Submission 5*, p. 37.

> reckless as to the harm to Australia's interests could properly be said to be in good faith.[35]

8.48 In addition, the Department identified:

> The sabotage offences only apply where a person intended to, or was reckless as to whether his or her conduct would, prejudice Australia's national security or advantage the national security of a foreign country (or, in relation to sections 82.7 and 82.8, to harm or prejudice Australia's economic interests, disrupt the functions of government or damage public infrastructure). A good faith defence is not appropriate.[36]

Consequential amendments

Telecommunications interception

8.49 Under Schedule 4 to the Bill, discussed in Chapter 10, enforcement agencies will be able to apply for a telecommunications interception warrant for the purposes of investigating any of the proposed offences in Division 82.

Citizenship

8.50 As discussed in Chapter 10, the Bill proposes expanding the current citizenship cessation regime to include all of the new sabotage offences proposed by the Bill, including the 'introducing vulnerability' offences in proposed sections 82.7 and 82.8. The Bill also proposes that a conviction for any of these offences will be grounds to refuse the citizenship application of a stateless person.

Deportation

8.51 Consequential amendments in Schedule 1 to the Bill, discussed in Chapter 10, affect the Minister's powers to deport a person convicted of a sabotage offence.

Committee comment

8.52 The Committee did not receive a large amount of evidence on the sabotage offences.

---

35 Attorney-General's Department, *Submission 6.1*, p. 9.

36 Attorney-General's Department, *Submission 6.2*, p. 5.

8.53 The Committee expressed initial concerns regarding the breadth of the definition of 'public infrastructure' in the Bill. Rather than being limited to 'critical' infrastructure, the definition may extend to almost any publicly or privately owned infrastructure, facility, premises, network or electronic system. However, the Committee accepts that infrastructure of importance to Australia's national security extends to some private infrastructure.

8.54 The Committee also acknowledges concerns that the term 'damage to public infrastructure' is defined very broadly. However, the Committee notes that the sabotage offences in proposed sections 82.3 to 82.6 contain the additional element that the person must intend, or be reckless to whether, their conduct prejudices Australia's national security or advantages the national security of a foreign country. The Committee considers that this additional element means that the offences at proposed sections 82.3 to 82.6 are proportional and appropriately targeted to the threat. The definition of 'national security' is considered at Chapter 3 of this report.

8.55 Unlike the other sabotage offences, proposed sections 82.7 and 82.8 do not only apply to circumstances where a person intends that, or is reckless as to whether, their conduct will prejudice Australia's national security, or advantage another country's national security. These offences will also apply if the person intends that, or is reckless as to whether, their conduct will

- harm or prejudice Australia's economic interests,
- disrupt the functions of the Government of the Commonwealth, of a State or of a Territory, or
- damage public infrastructure.

8.56 To ensure that the offences in the Bill are proportional and appropriately targeted, the Committee considers that proposed sections 8.27 and 82.8 should be limited to circumstances where a person intends that, or is reckless as to whether, their conduct will prejudice Australia's national security or advantage the national security of a foreign country.

Recommendation 53

8.57 Consistent with the other sabotage offences in the Bill, the Committee recommends that proposed sections 82.7 and 82.8 (introducing vulnerability with intention, or recklessness, as to national security) be amended to remove the following elements:

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

8.58 The Committee notes the Law Council of Australia's concerns that the 'preparing or planning sabotage' offence in proposed section 82.9 is not necessary in light of the existing incitement, conspiracy and attempt provisions in the *Criminal Code*. The inclusion of preparatory offences in the Bill is discussed in general terms in Chapter 3. In the case of section 82.9, however, the Committee accepts the need for an offence that captures actions preparatory to a sabotage offence beyond the existing provisions in the *Criminal Code*.

8.59 The Committee notes that the defence at proposed section 82.10 currently only covers people acting in their capacity as a public official. Given that the Bill's definition of public infrastructure includes a range of privately-owned infrastructure, the Committee considers it important that this defence be broadened to include conduct undertaken on behalf of a private owner or operator of infrastructure.

Recommendation 54

8.60 The Committee recommends that the defence at proposed section 82.10, in relation to the Bill's sabotage offences, be broadened to include conduct engaged in on behalf of a private owner or operator of infrastructure, in addition to public officials.

9. Treason, treachery and other threats to security

9.1 This chapter reviews the proposed new offences of

- treason,
- treachery,
- other threats to security, including:
  - advocating mutiny,
  - assisting prisoners of war to escape,
  - military style training involving foreign government principal,
  - interference with political rights and duties, and
- damage to Commonwealth property.

9.2 The new offences, the relevant sections and proposed penalties are set out below.

Table 9.1 Treason, treachery and other threats to security offences

New Offence	Section	Penalty
Treason	80.1AA	Life Imprisonment
Treachery	80.1AC	Life Imprisonment
Advocating mutiny	83.1	7 years
Assisting prisoners of war to escape	83.2	15 years
Military style training involving foreign government principal	83.3	20 years
Interference with political rights and duties	83.4	10 years

Damaging Commonwealth property	132.8A	10 years

Treason and treachery

Treason

9.3 Section 80.1AA of the Bill proposes to repeal the existing offence of 'Treason – materially assisting enemies' and replaces it with the offence 'Treason – assisting enemy to engage in armed conflict.'

9.4 The Explanatory Memorandum explains that the new treason offence will

> modernise Australia's treason offences. It will ensure that treason offences regarding assisting an enemy to engage in armed conflict against Australia, which carries a penalty of life imprisonment, appropriately reflect moderns terminology related to armed conflict.[1]

9.5 The new treason offence provides that a person commits an offence if:

- a party (the enemy) is engaged in armed conflict involving the Commonwealth or the Australian Defence Force, and
- the enemy is declared in a Proclamation made under section 80.1AB, and
- the person engages in conduct, and
- the person intends that the conduct will materially assist the enemy to engage in armed conflict involving the Commonwealth or the Australian Defence Force, and
- the conduct materially assists the enemy to engage in armed conflict involving the Commonwealth or the Australian Defence Force, and
- at the time the person engages in the conduct
  - the person knows that the person is an Australian citizen or a resident of Australia, or
  - the person knows that the person has voluntarily put himself or herself under the protection of the Commonwealth, or
  - the person is a body corporate incorporated by or under a law of the Commonwealth or of a State or Territory.

9.6 The offence has a maximum penalty of life imprisonment.

---

1 Explanatory Memorandum, p. 27.

9.7 In addition, proposed new section 80.1AB deals with the proclamation of enemy engaged in armed conflict, providing that:

> The Governor-General may, by Proclamation, declare a party to be an enemy engaged in armed conflict involving the Commonwealth or the Australian Defence Force [ADF].[2]

9.8 The Law Council of Australia was broadly supportive of the new treason offence, stating that it

> appreciates the necessity to update the treason offences as 'armed conflict' reflects the reality of the current international engagements of the ADF and Commonwealth (e.g. the fight against [Islamic State of Iraq and Syria] and the situation in Syria).[3]

9.9 However, the Law Council also raised concerns around the breadth of the offence, as it

> removes the requirement that the person's conduct assists a country or organisation engaged in hostilities *against* the Commonwealth or ADF. The proposed requirement is that a person's conduct provides material assistance to a country or organisation engaged in an armed conflict *involving* the Commonwealth. Given the multilateral nature of modern conflicts (see, for example, in the case of Syria), this makes the scope of the offence potentially very broad. Further, that someone contributes to acting against the Commonwealth or ADF would seem to be the rationale behind treason.[4]

9.10 Similarly, the joint councils for civil liberties argued that 'it is difficult to conceive of a situation appropriate to the triggering of a treason offence that could not be captured by maintaining the more specific "against"'.[5]

9.11 The joint councils for civil liberties and the Law Council proposed changing the word 'involving' to the word 'against' in the offence and in the Proclamation power.[6]

9.12 Responding to these recommendations, the Attorney-General's Department stated that:

---

2 Proposed section 80.1AB.

3 Law Council of Australia, *Submission 5*, p. 29.

4 Law Council of Australia, *Submission 5*, pp. 29-30 (emphasis in original).

5 Joint councils for civil liberties, *Submission 31*, p. 40.

6 Joint councils for civil liberties, *Submission 31*, p. 40; Law Council of Australia, *Submission 5*, p. 30.

> This would not be appropriate given the realities of modern armed conflict. It is entirely possible that the ADF may be engaged in an armed conflict involving multiple actors such as insurgent groups. The ADF may not necessarily be engaged in combat operations against all of the actors in such a context. It may, for example, be engaged in training, advising, and otherwise assisting missions in support of and with the consent of a foreign government, which would not see Australia engaged in combat 'against' an enemy. In such circumstances, Australia may still be a party to the armed conflict, in which case the conduct intended to be caught by this provision should still be criminalised.[7]

Materially assist

9.13 Both the current and proposed treason offence require the accused to intend to 'materially assist' an enemy. The term is not defined and will be given its ordinary meaning. The Explanatory Memorandum outlines that the term is intended to include:

- the provision of monetary assistances or practical goods, and
- assistance which is more than merely trivial.[8]

9.14 The Committee was interested in the use of the term 'materially assist' as opposed to language in the similar *Criminal Code* offence of 'Providing support to a terrorist organisation' (section 102.7), which refers to 'provides to an organisation support or resources'. The Committee asked the Attorney-General's Department why there was a difference in language used. The Department replied:

> The use of the term 'materially assist' is consistent with existing treason offences. It has been retained as it is a high threshold for the assistance that must be provided in order for a treason offence to be committed. It is a higher threshold than that found in the offence relating to terrorist organisations at section 102.7, which is considered appropriate given the severe penalty applying to treason offences.[9]

---

7 Attorney-General's Department, *Submission 6.1*, p. 6.

8 Explanatory Memorandum, p. 31.

9 Attorney-General's Department, *Submission 6.1*, p. 86.

Residents

9.15 The Explanatory Memorandum provides that, consistent with existing offences, the proposed offence

> ensures that a person only commits this offence if he or she knows that they owe an allegiance to the Commonwealth. This is appropriate because only persons who benefit from the protection of the Australian state should be able to commit treason against the Commonwealth.[10]

9.16 The current and proposed offence apply to all 'residents', defined in the *Criminal Code* as any 'individual who is a resident of Australia.' The Committee sought clarification on whether this term was intended to extend to persons staying in Australia on a temporary visa, for example a student visa, business visa or tourist visa, and if so, whether these persons owe an allegiance to Australia sufficient to engage in treason. The Attorney-General's Department advised that the Bill 'is not limited to permanent residents', explaining that 'a person who is voluntarily temporarily resident in Australia would be considered to have "voluntarily put himself or herself under the protection of the Commonwealth"'.[11]

Proclamations

9.17 The Governor-General may, by Proclamation, declare a party (a person, body or group of any kind) to be an enemy engaged in armed conflict involving the Commonwealth or the Australian Defence Force (section 80.1AB). The Law Council of Australia expressed concern that

> no criteria are prescribed for when a Proclamation may be made under this proposed section. Similarly, there is no requirement of periodic review of such a Proclamation or an ability of revocation.[12]

9.18 The Attorney-General's Department responded to this concern:

> [T]here would be no benefit in listing further criteria than are already contained in section 80.1AB. The question of whether a party is an enemy engaged in armed conflict involving the Commonwealth or the Australian

---

10 Explanatory Memorandum, p. 32.

11 Attorney-General's Department, *Submission 6.1*, p. 87.

12 Law Council of Australia, *Submission 5*, p. 30.

Defence Force will be determined based on expert advice in the context of the meaning of the terms in international law.[13]

9.19 The Law Council further recommended that there should be a requirement of periodic review of such a Proclamation and an ability of revocation when the Governor-General is no longer satisfied that the criterion for making the Proclamation continues to be met.[14]

9.20 The Department explained that as a Proclamation is a legislative instrument, 'it can be repealed through the usual processes'.[15] In addition it will sunset every ten years under the operation of the *Legislation Act 2013*, and as a result, this would ensure 'that such instruments are periodically reviewed and only re-made if required'.[16]

9.21 The *Acts Interpretation Act 1901* provides that a person who is authorised by an Act to make, grant or issue a legislative instrument also has a power to repeal the instrument.[17] The Governor-General would have the power to repeal the Proclamation by making another legislative instrument to that effect.

9.22 The Law Council also suggested that there should be a prohibition on the retrospective proclamation of a 'party to be an enemy engaged in armed conflict' under proposed section 80.1AB.[18]

9.23 Responding to the recommendation, the Department pointed to section 12(2) of the *Legislation Act 2003*,[19] which prevents retrospective application of a Proclamation made under section 80.1AB of the Bill.

---

13 Attorney-General's Department, *Submission 6.1*, pp. 6 - 7.

14 Law Council of Australia, *Submission 5*, p. 30.

15 Attorney-General's Department, *Submission 6.1*, p. 7.

16 Attorney-General's Department, *Submission 6.1*, p. 7.

17 9.1 The relevant provision is subsection 33(3) "Power to make instrument includes power to vary or revoke etc. instrument" *Where an Act confers a power to make, grant or issue any instrument of a legislative or administrative character (including rules, regulations or by laws) the power shall be construed as including a power exercisable in the like manner and subject to the like conditions (if any) to repeal, rescind, revoke, amend, or vary any such instrument.*

18 Law Council of Australia, *Submission 5*, p. 30.

19 Section 12(2) of the *Legislation Act 2013* provides that a legislative instrument or notifiable instrument does not apply in relation to a person (other than the Commonwealth or an authority of the Commonwealth) if the provision commences before the day the instrument is registered,

Consequential amendments

Presumption against bail

9.24 Consequential amendments in Schedule 1 to the Bill, discussed in Chapter 10, affect laws relating to the presumption against bail contained in section 15AA of the *Crimes Act 1914*. The Bill proposes imposing a new presumption against bail for treason offences.

Treachery

9.25 The Bill proposes to replace the existing 'Treachery' offence in section 24AA of the Crimes Act with a modernised offence in section 80.1AC of the *Criminal Code*. The Explanatory Memorandum provides:

> The new treachery offence will criminalise the use of force or violence intended to overthrow the Constitution, the Government of the Commonwealth or of a State or Territory or the lawful authority of the government of the Commonwealth.[20]

9.26 The new treachery offence provides that a person commits an offence if:

- the person engages in conduct, and
- the conduct involves the use of force or violence, and
- the person engages in the conduct with the intention of overthrowing
  - the Constitution, or
  - the Government of the Commonwealth, of a State or of a Territory, or
  - the lawful authority of the Government of the Commonwealth.

9.27 The offence has a maximum penalty of life imprisonment.

9.28 The amendments narrow the scope of the offence to exclude conduct against countries other than Australia and reduce overlap with treason offences. The Explanatory Memorandum states:

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

---

to the extent that as a result: (a) the person's rights as at that day would be affected so as to disadvantage the person; or b) liabilities would be imposed on the person in respect of anything done or omitted to be done before that day.

20 Explanatory Memorandum, p. 34.

> The existing treachery offence at subsection 24AA(2) is not being replicated in the new treachery offence because assisting enemies of the Australian Defence Force is covered by the treason offence in section 80.1AA, as inserted by Item 4 of Schedule 1.[21]

Lawful authority of the Government

9.29 In addition to overthrow of the Constitution, the Federal Government or a State Government, the offence would also extend to intended conduct to overthrow of the 'lawful authority of the Commonwealth Government' by use of force or violence. This term is not defined.

9.30 The Attorney-General's Department explained that the term 'is used for consistency with the existing offence of urging violence against the Constitution in section 80.2 of the *Criminal Code*',[22] and pointed to the Explanatory Memorandum, which states:

> For paragraph 80.1AC(1)(c), the prosecution will have to prove beyond a reasonable doubt that the person engaged in his or her conduct with the intention of overthrowing the Constitution, the Government of the Commonwealth or a State or Territory or the lawful authority of the Government of the Commonwealth. This could include the overthrow of an arm of the Government. If a person intended to overthrow the Executive Government then this will be sufficient even if they do not intend to overthrow the Parliament or the judiciary. The application of intention to this result element means that the prosecution will have to prove that the person means to bring about the overthrow or is aware that it will occur in the ordinary course of events.[23]

9.31 The existing offence that the Department refers to 'Urging violence against the Constitution' in section 80.2 of the *Criminal Code* has a penalty of imprisonment for seven years. At the time this offence was enacted concerns were raised around the 'vagueness'[24] of the term and the,

> … extent to which the 'lawful authority' of the Government must be challenged in order to constitute urging the 'overthrow' of the lawful

---

21 Explanatory Memorandum, p. 34.

22 Attorney-General's Department, *Submission 6.1*, p. 87.

23 Explanatory Memorandum, p. 35.

24 See Patrick Emerton quoted in Australian Law Reform Council, *Fighting Words: A Review of Sedition Laws in Australia (ALRC Report 104)*, tabled 13 December 2006, p. 189.

> authority of the Government. For example, is it sufficient that force or violence be urged to resist one or more specific laws, or must there be a more general challenge to the legitimacy of the Government?[25]

Force or violence

9.32 The Committee sought to clarify whether the reference to 'force or violence' in the proposed offence purposefully excludes intimidation or threats, concepts which are explicitly criminalised in the proposed 'interference with political rights and duties' offence. The Attorney-General's Department advised:

> The use of the term 'force or violence' picks up on the language used in the existing treachery offence at subparagraph 24AA(1)(a)(ii) of the Crimes Act. It is also consistent with the language used in the existing offence of urging violence against the Constitution in section 80.2 of the Criminal Code (see paragraph 80.2(1)(a)).
>
> Conversely, the references to intimidation and threats in new section 83.4 of the Bill pick up on the existing language used in section 28 of the Crimes Act.
>
> Given that a penalty of life imprisonment applies to the treachery offence at subsection 80.1AC of the Bill, it is considered appropriate that the offence be limited to conduct involving force or violence and not extend to conduct involving intimidation or threats.[26]

9.33 The Law Council of Australia raised a concern regarding the fault element that applies to the offence, stating that

> the fault element of intention should be required where the person engages in conduct involving the use of force or violence. That is, the person should be required to have intended to use force or violence given the potential penalty of life imprisonment.[27]

9.34 The Attorney-General's Department addressed this recommendation as follows:

> As drafted, the physical element is a circumstance element. Consistent with section 5.6 of the Criminal Code, recklessness is the automatic fault element

---

25 Australian Law Reform Council, *Fighting Words: A Review of Sedition Laws in Australia (ALRC Report 104)*, tabled 13 December 2006, p. 188.

26 Attorney-General's Department, *Submission 6.1*, pp. 87 -88.

27 Law Council of Australia, *Submission 5*, p. 31.

for a circumstance element. The Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers states (at page 20):

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

The department has not identified a reason to override the automatic fault element and apply intention to this element.[28]

Consequential amendments

Citizenship

9.35 Section 35A of the *Australian Citizenship Act 2007* enables the Minister to determine that a dual-citizen has ceased to be an Australian citizen in circumstances where the dual-citizen is convicted of a treachery offence against section 24AA of the *Crimes Act*, and other statutory criteria are met. Schedule 1 to the Bill, discussed in Chapter 10, amends section 35A of the *Australian Citizenship Act 2007* so as to apply to the proposed new treachery offences. The Bill also proposes that a conviction for the new treachery offence will be grounds to refuse the citizenship application of a stateless person.

Deportation

9.36 Consequential amendments in Schedule 1 to the Bill, discussed in Chapter 10, affect the Minister's powers to deport a person convicted of a treachery offence.

Presumption against bail

9.37 Consequential amendments in Schedule 1 to the Bill, discussed in Chapter 10, affect laws relating to the presumption against bail contained in section 15AA of the *Crimes Act 1914*. The offence of treachery set out in section 24AA of the *Crimes Act* is currently subject to section 15AA. The Bill proposes substituting this reference to the new treachery offence in proposed section 80.1AC.

---

[28] Attorney-General's Department, *Submission 6.1*, p. 7.

Standard non-parole periods

9.38 Section 19AG of the *Crimes Act* will continue to require minimum non-parole periods to be fixed in relation to all convictions for treachery offences. This matter is discussed in Chapter 10.

Committee comment

Treason

9.39 The Committee accepts the need to modernise the treason offence and has considered concerns that the offence should capture conduct 'against' rather than 'involving' the Commonwealth or the Australian Defence Force. However, the Committee notes the Attorney-General's Department's evidence on the 'realities of modern armed conflict' and concludes that the term 'involving' the Commonwealth or the Australian Defence Force is appropriate.

9.40 The Committee considered the provision for an enemy to be declared in a Proclamation made under proposed section 80.1AB. The Committee accepts that the making of such a Proclamation must be one which relies on expert evidence at the time and such a Proclamation power should not be fettered by additionally imposed legislative criteria.

9.41 The Committee also considered the Law Council of Australia's recommendation that there be a requirement of periodic review of Proclamations under proposed section 80.1AB, and an ability of revocation when the Governor-General is no longer satisfied that the criterion for making the Proclamation continues to be met. However, the Committee concludes that such amendments are not necessary. As noted above, a Proclamation by the Governor-General is a legislative instrument and can be repealed if necessary by virtue of sub-section 33(3) of the *Acts Interpretation Act 1901*. While there is no specific requirement that such a Proclamation be reviewed periodically, the proposed treachery offence in section 81.1AA can only be committed if a party is engaged in armed conflict involving the Commonwealth or the Australian Defence Force. This means that, in the event that peace or victory over the proclaimed enemy is declared, the elements of the offence would not likely be able to be established, even if the Proclamation remained in force.

Treachery

9.42 The Committee notes that the Bill proposes to replace the existing treachery offence in section 24AA of the Crimes Act and replace it with a modernised version in section 80.1AC of the Criminal Code. The Bill narrows the scope of the treachery offence to exclude conduct against countries other than Australia and to reduce overlap with treason offences.

9.43 Similarly to the existing offence, the new offence applies to the use of force or violence with the intention of overthrowing the Constitution, or the Government of the Commonwealth, of a State or of a Territory. The proposed new offence also extends to the use of force or violence with the intention of overthrowing the 'lawful authority of the Government of the Commonwealth'. To assist with ensuring the offence is clear and unambiguous in its terms, the Committee suggests that the Explanatory Memorandum could clarify the circumstances in which the term 'lawful authority of the Government of the Commonwealth' might apply.

Other threats to security

9.44 As noted above, Division 83 inserts four new offences into the *Criminal Code*. The four new offences, the relevant section and proposed penalty are set out below.

Table 9.2 Other threats to security—new offences

New Offence	Proposed section	Penalty
Advocating mutiny	83.1	7 years
Assisting prisoners of war to escape	83.2	15 years
Military style training involving foreign government principal	83.3	20 years
Interference with political rights and duties	83.4	10 years
Damaging Commonwealth property	132.8A	10 years

9.45 The offences are similar to existing offences in the *Crimes Act 1914*, outlined in the table below, which are repealed by Item 43 of Schedule 1 of the Bill.

Table 9.3 Other threats to security—existing offences

Existing Offence	Section in *Crimes Act 1914*	Penalty
Inciting mutiny	25	Imprisonment for life
Assisting prisoners of war to escape	26	Imprisonment for life
Unlawful drilling	27	5 years
Interference with political liberty	28	3 years
Destroying or damaging Commonwealth property	29	10 years

Consequential amendments

Citizenship applications

9.46 Schedules 1 and 2 to the Bill, discussed in Chapter 10, also contain amendments to the definition of 'national security offence' in section 3 of the *Australian Citizenship Act 2007*, which affects the treatment of applications for Australian citizenship made by stateless persons. The offences set out in Table 9.3 are currently defined as a 'national security offence' for this purpose. The Bill proposes substituting these references to the new forms of these offences set out in Table 9.2 above, with the exception of the offence of damaging Commonwealth property, which will no longer be deemed to be a 'national security offence'.

Advocating mutiny

9.47 Section 83.1(1) of the Bill provides that:

> (1) A person (the advocate) commits an offence if:
>
> (a) the advocate engages in conduct; and 4 (b) the conduct involves advocating mutiny; and
>
> (c) the advocate engages in the conduct reckless as to whether the result will be that a defence member (within the meaning of the *Defence Force Discipline Act 1982*) will take part in a mutiny; and (d) at the time the advocate engages in the conduct:

(i) the advocate knows that the advocate is an Australian citizen or a resident of Australia; or

(ii) the advocate knows that the advocate has voluntarily put himself or herself under the protection of the Commonwealth; or

(iii) the advocate is a body corporate incorporated by or under a law of the Commonwealth or of a State or Territory.

9.48 Section 83.1 (advocating mutiny) updates the language used in section 25 (inciting mutiny) of the *Crimes Act 1914*. It includes a definition of mutiny as follows:

> A mutiny is a combination between persons who are, or at least 2 of whom are, members of the Australian Defence Force:
>
> (a) to overthrow lawful authority in the Australian Defence Force or in a force of another country that is acting in cooperation with the Australian Defence Force; or
>
> (b) to resist such lawful authority in such a manner as to substantially prejudice the operational efficiency of the Australian Defence Force or of, or of a part of, a force of another country that is acting in cooperation with the Australian Defence Force.[29]

9.49 The Explanatory Memorandum states that:

> The term 'advocate' is not defined and is intended to take its ordinary meaning, including to counsel, promote, encourage or urge the commission of a mutiny. The ordinary meaning of each of the relevant expressions varies, but it is important that they be interpreted broadly to ensure a person who advocates mutiny does not escape punishment by relying on a narrow construction of the terms or one of the terms.[30]

9.50 The breadth of the term is shown by the example offence in the Explanatory Memorandum:

> An example of this offence is as follows. Person A is an Australian citizen and is married to a member of the Australian Defence Force. Person A is aware that his spouse is unhappy in her role and encourages his spouse to convince other members of the Australian Defence Force to resist orders from their

[29] Proposed section 83.1(2).

[30] Explanatory Memorandum, p. 78.

> superiors so that a particular Defence operation against one of Australia's enemies cannot take place.[31]

9.51 'Advocating mutiny' will have broader application than the existing 'inciting mutiny offence', and some submitters considered it could potentially capture citizens offering peaceful protest against Australian military action. Valerie Heath submitted that the offence

> could have the effect of criminalising any peaceful advocacy by civilians against Australian involvement in wars or warlike activity or peaceful advocacy that Australian servicemen and women apply the Nuremburg principle in considering the lawfulness of orders they have been given. No policy case has been raised by the Executive that would support such a change.[32]

9.52 The Law Council of Australia identified that 'the breadth of the provision may not be compatible with the right to freedom of opinion and expression'. In indicating its opposition to the offence, the Law Council stated:

> an updated inciting mutiny offence in the Criminal Code replacing section 25 of the Crimes Act would be preferable. Incitement, conspiracy and attempt provisions in Part 2.4 of the Criminal Code should instead be relied on. If this is not to be accepted, the Law Council recommends that the fault element of intention rather than recklessness should apply as to whether the person's words or conduct will cause another person to engage in mutiny.[33]

9.53 At a public hearing, the Law Council reiterated its view that the existing mechanisms in the *Criminal Code* should be used for the offence, rather than introducing the term 'advocate'.[34]

Penalty

9.54 The penalty for advocating mutiny has been reduced to seven years imprisonment from the life imprisonment contained in section 25 of the *Crimes Act 1914*.

---

31 Explanatory Memorandum, p. 76.

32 Valerie Heath, *Submission 14*, p. 1.

33 Law Council of Australia, *Submission 5*, p. 39.

34 Dr David Neal SC, Member, National Criminal Law Committee, Law Council of Australia, *Committee Hansard*, Melbourne, 16 March 2018, p. 11.

Defence

9.55 As drafted the Bill contains no defence to the offence of advocating mutiny.

9.56 In relation to the proposed offence for advocating mutiny, the Law Council of Australia recommended the provision of a good faith defence

> to ensure that individuals or groups who in good faith with their words oppose the actions of the ADF or a defence force of another country that is acting in cooperation with the ADF and calls for a laying down of arms is not subject to the offence.[35]

9.57 The Attorney-General's Department did not oppose the Law Council's recommendation, commenting:

> The Bill could be amended to provide that the good faith defence at section 80.3 of the Criminal Code is available for the offence of advocating mutiny. This would mean that the offence does not apply if a person engages in a limited range of conduct undertaken in good faith.[36]

9.58 It is noted that, should such a defence be made available, section 83.5(4) 'Consent of Attorney-General required for prosecutions' would need to be amended so that the Attorney-General must consider whether conduct might be authorised in a way mentioned in section 80.3.

Assisting prisoners of war to escape

9.59 Proposed section 83.2 (assisting prisoners of war to escape) updates the language used in the identically named offence section 26 of the Crimes Act. Specifically, it updates the definition of prisoner of war to be that 'within the meaning of Article 4 of the Third Geneva Convention'. In addition, the person must be in custody 'wholly or partly by the Commonwealth or the Australian Defence Force' and that the conduct 'takes place in the context of an international armed conflict'.

Penalty

9.60 The penalty for assisting prisoners of war to escape has been reduced to 15 years imprisonment from the existing penalty of life imprisonment

---

35 Law Council of Australia, *Submission 5*, p. 39.

36 Attorney-General's Department, *Submission 6.1*, p. 10.

contained in section 26 of the Crimes Act. The Explanatory Memorandum notes that

> Section 26 of the Crimes Act was enacted in the original Crimes Act in 1914 and the existing penalty of life imprisonment does not reflect contemporary standards of seriousness.[37]

9.61 The Law Council of Australia pointed out that an element of the offence under proposed section 83.2 is that 'the conduct assists one or more prisoners of war (within the meaning of Article 4 of the Third Geneva Convention) to escape from custody'. Given the Bill refers to provisions of the Third Geneva Convention, they are, the Law Council argued, directly relevant to the interpretation of this provision. Taking this into account the Law Council argued for a reduction in the penalty as follows:

> The Third Geneva Convention stipulates that a prisoner of war should not be punished for a successful escape, and that a prisoner of war captured in the process of escaping, if punished, should only be liable to a disciplinary punishment. In the Law Council's view, it would be inconsistent with the Third Geneva Convention to make assisting a prisoner of war to escape a criminal offence liable to imprisonment for 15 years.

9.62 The Attorney-General's Department noted that the offence is 'not directed at the actions of prisoners of war', stating:

> Given that the offence does not criminalise the acts of prisoners of war but rather persons who assist prisoners of war to escape, it would not be appropriate for the penalty to be lowered based on the obligations in the Third Geneva Convention as the Law Council has suggested.

Defence

9.63 There are no proposed defences to the offence of assisting prisoners of war to escape. No submitters suggested a defence be made available.

Military style training involving foreign government principal

9.64 Proposed section 83.3 (military style training involving foreign government principal) is currently known as 'unlawful drilling' in section 27 of the Crimes Act. The section provides that:

> (1) A person commits an offence if:

---

37 Explanatory Memorandum, p. 84.

(a) the person provides, receives, or participates in, training, and

(b) the training involves using arms or practising military exercises, movements or evolutions, and

(c) any of the following circumstances exists:

(i) the training is provided on behalf of a foreign government principal within the meaning of Part 5.2 (see section 90.3),

(ii) the training is directed, funded or supervised by a foreign government principal or a person acting on behalf of a foreign government principal.[38]

9.65 The Explanatory Memorandum gives an example of the offence as follows:

> Person A participates in training in Australia which is provided by Country E. The training involves the use of weapons and military-style drills. Country E is undertaking the training at a hidden rural location and intends for the training to assist it to conduct military operations against Country F, a close neighbour of Australia. Person A is intending to participate in those future military operations against Country F.[39]

9.66 The proposed section also offers defences to prosecution where the conduct is either

- authorised by written agreement, or
- solely for service with armed force other than terrorist organisation.[40]

9.67 The Law Council of Australia noted that

> a State that is responsible for directing, funding or supervising training of the nationals of a second State for the purposes of acting against that second State violates the principle of non-intervention and therefore may amount to an internationally wrongful act.[41]

and that

> [a]n Australian domestic court is unable to make a finding against a foreign State under the principle of sovereignty at international law. Nonetheless, the

38 Proposed section 83.3.

39 Explanatory Memorandum, p. 84.

40 Proposed paragraphs 83.3(2) and 83.3(3)–(4).

41 Law Council of Australia, *Submission 5*, p. 42.

> Law Council encourages the Committee to inquire into the possible impact at international law as to whether a finding by an Australian court for the purposes of this offence may amount to *opinio juris* at international law.[42]

9.68 The Attorney-General's Department addressed this concern of the Law Council and stated that:

> these issues will not be relevant to a determination of individual criminal responsibility for the purposes of this offence …
>
> A decision of an Australian court may constitute evidence of either State Practice or *opinio juris*, which are the two elements required to demonstrate the existence of a customary international law norm. In both instances, however, evidence of one country's practice or sense of obligation will be insufficient to demonstrate a rule of customary international law. There must be sufficiently widespread and representative practice among countries accompanied by a sense of legal obligation.[43]

Possible unintended effect on humanitarian agencies

9.69 The Law Council of Australia and a joint submission by the International Committee of the Red Cross and the Australian Red Cross raised concerns in relation to the effect the offence of military style training involving foreign government principal may have on their humanitarian work.[44]

9.70 The Law Council submitted:

> As presently drafted, the offence is too broad, as it applies to a person who 'provides, receives, or participates in, training' and 'the training involves using arms or practising military exercises, movements or evolution' provided by a foreign principal without the requirement for that training to be directed towards a predetermined hostile act nor for it to form an integral part of that act.[45]

9.71 The joint submission by the International Committee of the Red Cross and the Australian Red Cross outlined the humanitarian work their organisations undertake, explaining that they support

---

42 Law Council of Australia, *Submission 5*, p. 42.

43 Attorney-General's Department, *Submission 6.1*, p. 11.

44 See Law Council of Australia, *Submission 5*, pp. 41-42 and International Committee of the Red Cross and the Australian Red Cross, *Submission 21*.

45 International Committee of the Red Cross and the Australian Red Cross, *Submission 21*, p. 3.

> the efforts of armed forces and groups to disseminate international humanitarian law and international human rights law and to integrate these norms into their doctrine, education and training. These activities allow us to bring a humanitarian perspective to military training environments, and to ensure that participants understand the rules that limit suffering in war and that they are obliged by law to adhere to those rules. They are also part of our ongoing dialogue with armed actors to ensure security and access for future humanitarian operations.[46]

9.72 Further, the submission raised the concern that, as it is currently drafted, the offence in section 83.3 could apply to the International Committee of the Red Cross and the Australian Red Cross' humanitarian activities. The submission elaborated:

> [T]he Explanatory Memorandum's example of conduct engaging the offence suggests that the provision is not intended to capture the kind of humanitarian activities outlined above. We recommend that this be made explicit, preferably by way of an exception, or alternatively a defence, to remove the considerable risk that humanitarian actors are, prima facie, exposed to criminal liability.[47]

Penalty

9.73 The penalty for military style training involving foreign government principal has been increased to 20 years imprisonment from the five years contained in section 27 of the *Crimes Act 1914*.[48]

9.74 The Explanatory Memorandum justifies this as follows:

> The maximum penalty of 20 years imprisonment is comparable with maximum penalties for offences for providing or receiving training connected to terrorist acts which carry penalties of 15 and 25 years imprisonment. The maximum penalty is appropriate to recognise the serious harm to Australia's sovereignty, national security and other defence interests that could result

---

46 Law Council of Australia, *Submission 5*, pp. 41-42.

47 International Committee of the Red Cross and the Australian Red Cross, *Submission 21*, p. 3.

48 The existing offence of 'unlawful drilling' under section 27 the *Crimes Act 1914* carries a maximum penalty of imprisonment for 5 years for a person who 'trains or drills any other person to the use of arms or the practice of military exercises, movements, or evolutions' in contravention of the directions of a proclamation, or is 'present at any meeting or assembly of persons' for the purpose of such training or drilling. The maximum penalty is imprisonment for 2 years for a person who is trained or drilled at such a meeting or assembly.

> from the provision and receipt of military style training by a foreign government principal.[49]

Defence

9.75 There are two defences to prosecution for this offence as follows:

- authorised by written agreement (subsection 83.3(2)), and
- solely for service with armed force other than terrorist organisation (subsection 83.3(3)).

9.76 The Explanatory Memorandum points out that the defence at subsection 83.3(2) could apply:

> where members of the Australian Defence Force are permitted through a memorandum of understanding to undertake training of the kind described at subsection 83.3(1) with the military forces of a foreign government.[50]

Interference with political rights and duties

9.77 Section 83.4 (interference with political rights and duties) is currently known as 'interference with political liberty' as per section 28 of the *Crimes Act 1914*.

9.78 The proposed offence in section 83.4 arises where a person engages in conduct and

- the conduct involves the use of force or violence, or intimidation, or the making of threats of any kind, and
- the conduct results in interference with the exercise or performance, in Australia by any another [sic] person, of an Australian democratic or political right or duty, and
- the right or duty arises under the Constitution or a law of the Commonwealth.

9.79 The existing offence in section 28 of the *Crimes Act 1914* does not refer to the Commonwealth Constitution. Section 28 states:

> Any person who, by violence or by threats or intimidation of any kind, hinders or interferes with the free exercise or performance, by any other person, of any political right or duty, commits an offence.[51]

---

49 Explanatory Memorandum, p. 88.

50 Explanatory Memorandum, p. 88.

51 *Crimes Act 1914*, s. 28.

9.80 The Law Council of Australia outlined the differences in the proposed offence in comparison with the offence in section 28 of the *Crimes Act 1914*:

- 'use of force' is a broader concept than 'violence' and may, as the Explanatory Memorandum indicates, capture 'acts such as restraining, manipulating, coercing and physically making a person do something against their will'. The Law Council considers that the expansion to conduct involving the use of force is appropriate;
- the current offence has as a result that the conduct 'hinders or interferes with the free exercise or performance, by any other person, of any political right or duty' (emphasis added). In contrast, the new offence is limited to the result of 'interference with' the exercise or performance, in Australia by any another person, of an Australian democratic or political right or duty where that right or duty arises under the Constitution or a law of the Commonwealth. The concept of 'interference' is arguably broader than 'hinders'. The Law Council does not oppose the removal of the term 'hinders' in the new offence;
- interference must be to an 'Australian democratic or political right or duty where that right or duty arises under the Constitution or a law of the Commonwealth'. The Law Council supports this amendment…[52]

9.81 The Law Council also noted:

> The Explanatory Memorandum to the Bill does not address the intersection between the proposed new offence and contempt of Parliament. Presumably section 4C of the Crimes Act may apply to ensure that a Member of Parliament may not be punished twice for the one act or omission but this should be clarified in the Explanatory Memorandum.[53]

9.82 The Attorney-General's Department advised that

> nothing in the Bill affects the Parliament's powers in relation to contempt. The department agrees with the Law Council that section 4C of the Crimes Act will operate to prevent double jeopardy.[54]

---

52 Law Council of Australia, Submission 5, p. 43.

53 Law Council of Australia, *Submission 5*, pp. 43-44.

54 Attorney-General's Department, *Submission 6.1*, p. 12.

Penalty

9.83 The penalty for interference with political rights and duties has been increased to ten years imprisonment from the three years contained in section 27 of the *Crimes Act 1914*.

9.84 In relation to this increase in penalty, the Law Council of Australia was of the view that

> clear reasons for the increase from a 3 year to 10 year maximum penalty have not been given. In the absence of a clear justification, the proposed maximum term is too high.[55]

9.85 The Explanatory Memorandum states that a ten year maximum imprisonment term 'is appropriate and appropriately criminalises conduct involving force or violence that [interferes] with a person's exercise of their democratic or political rights or duties'.[56]

Defence

9.86 The Note to subsection 83.4(1) clarifies that the defence for acts of done in good faith at subsection 80.3 applies to the offence at section 83.4.[57]

Damaging Commonwealth property

9.87 Damage to Commonwealth property is currently covered by section 29 of the *Crimes Act 1914*, which provides:

> Destroying or damaging Commonwealth property
>
> (1) Any person who intentionally destroys or damages any property, whether real or personal, belonging to the Commonwealth or to any public authority under the Commonwealth, commits an offence.
>
> Penalty: Imprisonment for 10 years.
>
> (2) For the purposes of an offence against subsection (1), absolute liability applies to the physical element of circumstance of the offence, that the

---

55 Law Council of Australia, *Submission 5*, p. 44.

56 Explanatory Memorandum, p. 93.

57 Explanatory Memorandum, p. 93. Item 5 amends subsection 80.3(1) of the *Criminal Code* to insert the words 'and section 83.4' after the words 'Subdivisions B and C'. The effect of this amendment is to apply the defence for acts done in good faith in section 80.3 to the new offence of 'Interference with political rights and duties' in new section 83.4.

property is property belonging to the Commonwealth or to any public authority under the Commonwealth.

9.88 The new offence in section 132.8A (damaging Commonwealth property) reads as follows:

(1) A person commits an offence if:

(a) the person engages in conduct; and

(b) the conduct results in damage to, or the destruction of, property; and

(c) the property belongs to a Commonwealth entity.

Penalty: Imprisonment for 10 years.

(2) Absolute liability applies to paragraph (1)(c).

(3) Section 15.4 (extended geographical jurisdiction—category D) applies to an offence against this section.

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

- the person intentionally engaged in conduct,
- the person's conduct results in damage to, or the destruction of, property and the person is reckless as to this element, and
- the property belongs to a Commonwealth entity.[58]

9.90 This differs from the existing offence of 'destroying or damaging Commonwealth property' at section 29 of the Crimes Act, where the offence applies only if the person *intentionally* destroys or damages the property.

9.91 In relation to this being a category D offence—that is, applying to conduct outside Australia[59]—the Explanatory Memorandum states:

---

58 Explanatory Memorandum, p. 208.

59 Section 15.4 of the *Criminal Code* provides 'If a law of the Commonwealth provides that this section applies to a particular offence, the offence applies:

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

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

> Category D jurisdiction is appropriate because property belonging to a Commonwealth entity could be located outside of Australian territory. A common example is Australian Embassies and High Commissions located overseas. The application of Category D jurisdiction is also consistent with other Commonwealth property offences in Part 7.2 of the Criminal Code, including the theft offence at section 131.1.[60]

9.92 The Law Council of Australia considered that

> the proposed damaging Commonwealth property offence is more appropriately framed in accordance with the *Criminal Code* model than the existing offence of destroying or damaging Commonwealth property at section 29 of the Crimes Act.[61]

Penalty

9.93 The penalty for the proposed new offence is ten years imprisonment. This is unchanged from the existing offence. The Explanatory Memorandum states:

> The maximum penalty of 10 years imprisonment is appropriate and consistent with the existing penalty for the offence of destroying or damaging Commonwealth property in section 29 of the Crimes Act. The maximum penalty also complements comparable offences in other Commonwealth legislation. For example, the offence of unauthorised modification of data to cause impairment at subsection 477.2 of the Criminal Code has a maximum penalty of 10 years imprisonment.[62]

Defence

9.94 There are no specific defences to this offence.

Committee comment

9.95 The Committee received limited evidence regarding the new offences relating to 'other threats to security'.

9.96 For the offence of 'advocating mutiny' in proposed section 83.1, the Committee notes that the term 'advocating' is not defined and is intended to take its ordinary meaning. However, the Committee notes that the description of the term in the Explanatory Memorandum uses the same

---

60 Explanatory Memorandum, p. 210.

61 Law Council of Australia, *Submission 5*, p. 54.

62 Explanatory Memorandum, p. 210.

language as in the existing *Criminal Code* definition of 'advocate' for the purpose of the 'advocating terrorism' offence in section 80.2C:

> ***advocates***: a person ***advocates*** the doing of a terrorist act or the commission of a terrorism offence if the person counsels, promotes, encourages or urges the doing of a terrorist act or the commission of a terrorism offence.[63]

9.97 The term is also defined for the purpose of the 'advocating genocide' offence in section 80.2D in the *Criminal Code*, using the same language ('counsel, promote, encourage or urge').

9.98 Consistent with these similar offences, and in line the Committee's requirement for the Bill to be clear and unambiguous in its terms, the Committee recommends that the term 'advocate' should be similarly defined for the purpose of the 'advocating mutiny' offence at proposed section 83.1.

Recommendation 46

9.99 **The Committee recommends that the Bill be amended to define the term 'advocating' for the purpose of proposed section 83.1 (advocating mutiny), consistent with other existing offences in the *Criminal Code*.**

9.100 In its report on the Counter Terrorism Legislation Amendment (Foreign Fighters) Bill 2014, the Committee accepted that 'recklessness' was the appropriate test for assessing an individual's behaviour under the proposed 'advocating terrorism' offence.[64] The Committee notes the proposed offence is 'advocating mutiny' as opposed to 'inciting mutiny', and similarly accepts that recklessness is the appropriate test for assessing an individual's behaviour under the offence.

9.101 In its 2014 report, the Committee also considered that the existing 'good faith' defence and other criminal law safeguards in relation to 'advocating terrorism' would ensure an appropriate balance was struck between free speech, healthy public discourse and the illegal and unwanted encouragement of terrorism.[65] The Committee similarly believes that

---

63 *Criminal Code*, section 80.2C(3) (emphasis in original)

64 Parliamentary Joint Committee on Intelligence and Security, *Advisory report on the Counter Terrorism Legislation Amendment (Foreign Fighters) Bill 2014*, October 2014, p. 39.

65 Parliamentary Joint Committee on Intelligence and Security, *Advisory report on the Counter Terrorism Legislation Amendment (Foreign Fighters) Bill 2014*, October 2014, p. 43.

providing a 'good faith' defence in relation to the offence of advocating mutiny will provide an appropriate balance between free speech, healthy public discourse and the illegal and unwanted encouragement of mutiny.

9.102 The Committee, therefore, recommends that the Bill be amended to provide that the good faith defence at section 80.3 of the *Criminal Code* is available for the proposed advocating mutiny offence.

Recommendation 47

9.103 **The Committee recommends that the Bill be amended to provide that the 'good faith' defence at section 80.3 of the *Criminal Code* is available for the offence of advocating mutiny.**

9.104 Consequential to this recommendation, the Committee recommends that proposed section 83.5(4) 'Consent of Attorney-General required for prosecutions' be amended so that, for an offence against section 83.1, the Attorney-General must consider whether conduct might be authorised in a way mentioned in section 80.3.

Recommendation 48

9.105 **The Committee recommends that proposed section 83.5(4) 'Consent of Attorney-General required for prosecutions' be amended so that, for an offence against section 83.1 (advocating mutiny), the Attorney-General must consider whether conduct might be authorised in a way mentioned in section 80.3.**

9.106 The Committee supports the inclusion of an updated offence in proposed section 83.2 for 'assisting prisoners of war to escape', and notes the substantial reduction in its maximum penalty from life imprisonment to 15 years in line with 'contemporary standards of seriousness'.

9.107 In relation to the offence of 'military style training involving foreign government' in proposed section 83.3, the Committee notes the concerns of the Law Council, and the International Committee of the Red Cross and the Australian Red Cross, that there could be a possible unintended effect on the work of humanitarian agencies.

9.108 The Committee previously discussed the issue of humanitarian aid in its report *Review of the 'declared area' provisions: Sections 119.2 and 119.3 of the Criminal Code* where it stated that:

> Given the important role of organisations such as the International Red Cross Red Crescent Movement in conflict environments, the Committee considers deterring such organisations from operating in declared areas to be beyond the intention of the legislation. The Committee recommends that this matter be clarified.[66]

9.109 The Committee made the following recommendation:

> The Committee recommends that section 119.2(3) of the *Criminal Code* be amended to make clear that humanitarian work beyond direct aid, including compliance training on the laws of armed conflict, is considered to be a 'legitimate purpose' for entering, or remaining in, a declared area.[67]

9.110 The Committee does not consider that the proposed offence is intended to impact on legitimate humanitarian work. The Committee recommends that this be made clear in the Bill by the provision of a defence in section 83.3 for those engaged in humanitarian work, including compliance training on the laws of armed conflict.

Recommendation 49

9.111 **The Committee recommends that proposed section 83.3 (military style training involving foreign government) be amended to provide a defence against prosecution for those engaged in humanitarian work, including compliance training on the laws of armed conflict.**

9.112 In relation to the intersection between the proposed offence of 'interference with political rights and duties' (section 83.4) and contempt of Parliament, the Committee notes that the Attorney-General's Department and the Law Council of Australia agreed that nothing in the Bill affects the Parliament's powers in relation to contempt. The Committee recommends that this matter be made clear in the Explanatory Memorandum.

9.113 The Committee notes that interference with political rights and duties using force of violence, intimidation or other threats is potentially a very serious matter. However, the Committee notes that no reasons are provided in the Explanatory Memorandum for the increase in maximum penalty from three

---

66 Parliamentary Joint Committee on Intelligence and Security, *Review of the 'declared area' provisions: Sections 119.2 and 119.3 of the Criminal Code*, p. 38.

67 Parliamentary Joint Committee on Intelligence and Security, *Review of the 'declared area' provisions: Sections 119.2 and 119.3 of the Criminal Code*, p. 38.

years' imprisonment under the existing offence to 10 years' imprisonment under the revised offence.[68] The Committee recommends that the Government reconsider whether this increase in penalty is necessary and proportionate.

Recommendation 50

9.114 **The Committee recommends that the Government reduce the penalty for the offence of 'interference with political rights and duties' at proposed section 83.4 from 10 years' imprisonment.**

Recommendation 51

9.115 **The Committee recommends that the Explanatory Memorandum be amended to clarify that nothing in the Bill affects the Parliament's powers in relation to contempt.**

9.116 In relation to the proposed offence for 'damaging Commonwealth property' at section 132.8A, the Committee notes that the offence largely uses similar elements to the existing offence in the Crimes Act, but is framed in accordance with the *Criminal Code* model. The Committee notes that, under this model, a person will not need to intend their conduct to result in damage to, or the destruction of, Commonwealth property to commit the offence. Rather, they will need to be reckless as to this outcome.

68 Explanatory Memorandum, p. 93.

10. Schedules 3 to 5 and consequential amendments

10.1 This chapter discusses the following amendments proposed in Schedules 3 to 5 to the Bill:

- a proposed new aggravated offence for giving false or misleading information in relation to a security clearance (Schedule 3),
- proposed amendments to the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) to enable telecommunications interception warrants to be requested in relation to the offences in the Bill (Schedule 4), and
- amendments to the *Foreign Influence Transparency Scheme Act 2018* that are proposed to come into effect if and once the Foreign Influence Transparency Scheme Bill 2017 and the Electoral Legislation Amendment (Electoral Funding and Disclosure Reform) Bill 2017 are passed by the Parliament.

10.2 This chapter also discusses a number of consequential amendments contained in Schedules 1 and 2 to the Bill, including amendments affecting:

- cessation of Australian citizenship,
- applications for Australian citizenship,
- deportation of non-citizens,
- presumption against bail, and
- in-camera court proceedings.

10.3 Finally, this chapter discusses the application of mandatory non-parole periods to many of the new offences created in the Bill.

Schedule 3 – Aggravated offence for giving false or misleading information

10.4 Schedule 3 will amend Division 137 of the *Criminal Code* to introduce a new aggravated offence for providing false or misleading information. The maximum penalty for the existing underlying offence is 12 months imprisonment. The maximum penalty for the proposed aggravated offence will be imprisonment for five years.[1]

Scope of the offence

10.5 Currently, it is an offence to knowingly provide information that is false or misleading to the Commonwealth, or to knowingly provide information which omits a matter so as to make the information provided misleading.[2] The Bill proposes creating an aggravated offence where the false or misleading information or omission is made in connection with the application for, or the maintenance of, an Australian Government security clearance.

10.6 The Explanatory Memorandum states that the proposed offence reflects the higher level of culpability and the serious consequences that can flow from providing misleading information in the context of the security clearance process.[3] The Explanatory Memorandum provides two scenarios in which the proposed aggravated offence would apply: where a vetting applicant does not disclose that they have previously participated in military service for a foreign country; and where a security clearance holder does not disclose that they have an ongoing association with an employee of a foreign government.[4]

10.7 In addition to the scenarios outlined by the Explanatory Memorandum, the proposed aggravated offence would also apply to any other person who provides information as part of the security clearance process, for example, the vetting candidate's personal referee or former employer. The Attorney-General's Department submitted that 'protecting the integrity of security

1 *Criminal Code*, section 137.1(1).

2 *Criminal Code*, section 137.1.

3 Explanatory Memorandum, p. 4.

4 Explanatory Memorandum, p. 295.

vetting is of fundamental importance and referee checking is a key element of the vetting process'.[5]

10.8 The Law Council of Australia expressed concern that the offence would capture a broader range of conduct than undeclared links to foreign principal. The Law Council gave the example of a vetting applicant omitting a singular incident of recreational drug use as conduct that could fall within the scope of the proposed aggravated offence.

10.9 The Law Council recommend that the proposed aggravated offence should not proceed, and instead suggested:

- an offence of failing to disclose defined activities linked to a foreign country or foreign principal in relation to an application for, or the maintenance of, an Australian Government security clearance; or alternatively
- the proposed aggravated offence should be limited to activities linked to a foreign country or foreign principal in relation to an application for, or the maintenance of, an Australian Government security clearance.[6]

10.10 The Law Council submitted that the scope of the proposed aggravated offence should reflect the intent of the Bill—to limit foreign adversaries from wielding undue influence.[7] The Attorney-General's Department responded to this concern as follows:

> Security clearance processes are not only concerned with a person's foreign association. They are intended to identify a range of potential vulnerabilities that may indicate that a person is not suitable to have access to classified information.
>
> The provision of false or misleading information about a person's personal or financial circumstances can be just as important as the person's connections to a foreign country when determining a person's suitability to hold a security clearance.[8]

---

5 Attorney-General's Department, *Submission 6.1*, p. 91.

6 Law Council of Australia, *Submission 5*, p. 72.

7 Law Council of Australia, *Submission 5*, p. 72.

8 Attorney-General's Department, *Submission 6.1*, p. 24.

Definition of key terms

10.11 As discussed in Chapter 3, the phrase 'Australian Government security clearance' is not defined in the Bill but is intended to capture the four clearances level outlined in the *Protective Security Policy Framework*: Baseline, Negative Vetting Level 1, Negative Vetting Level 2 and Positive Vetting.[9] The phrase 'maintenance' is also not defined in the Bill, nor does the Explanatory Memorandum outline the intended scope of activities and conduct that is sought to be characterised as constituting the 'maintenance of an Australian Government security clearance'.

Defences

10.12 The existing defences available to the underlying offence in section 137.1 will also apply to the proposed aggravated offence. The defence may be available where:

- the information provided is not false or misleading in a material particular;
- the information omitted did not omit any matter or thing without which the information is misleading in a material particular; or
- the Commonwealth does not take reasonable steps to inform the person providing the information, prior to their provision of the information, of the existence of the offence. For this purpose the *Criminal Code* provides that the officer can inform the person that 'giving false or misleading information is a serious offence'.[10]

Telecommunications interception

10.13 The Bill also proposes enabling law enforcement agencies to obtain a telecommunications interception warrant to investigate the proposed aggravated offence. The expansion of telecommunications interception powers is addressed in Chapter 10.

Committee Comment

10.14 The Committee recognises the significant harm that could be caused by a person acquiring or maintaining an Australian Government Security Clearance on the basis of an undeclared relationship to a foreign principal,

---

9 Explanatory Memorandum, pp. 132, 271.

10 *Criminal Code*, section 137.1(2)-(6).

or concealed allegiance to a foreign country. This information can be key to the Government's assessment of whether a person is suitable to hold a clearance, and if so, whether any risk mitigation strategies should be implemented. Accordingly, the Committee recognises the need to deter misleading conduct and to enable law enforcement agencies to effectively investigate it.

10.15 The Committee also recognises concerns that a broader range of conduct will fall within the ambit of the proposed offence than concealed foreign allegiances. Any type of information and any person providing such information, including personal referees, will be captured. The Committee notes the Attorney-General's Department's view that this is necessary because a person's personal or financial circumstances can be 'just as important' as their connections to foreign countries when determining whether a person is suitable to hold a clearance.[11]

10.16 However, the Committee also recognises that information provided by a referee, particularly for high-level security clearances, can be of an acutely personal nature. For example, a personal referee may have shared a sexual or romantic relationship with the security clearance holder, or may have engaged in criminal activity or drug taking with a security clearance applicant.

10.17 The Committee notes that all of the defences to the underlying offence in section 137.1 are available in connection with proposed new section 137.1A. This includes that the person does not commit an offence if the information is not false or misleading in a 'material particular', or if the Commonwealth entity (in this case, a security vetting authority) did not take reasonable steps to notify the person of the existence of the offence.

10.18 The Committee also notes that the default mental element of recklessness applies in relation to proposed section 137.1A(1)(b)—that is, the person must be aware of a substantial risk that they are giving the information in relation to an application for, or the maintenance of, an Australian Government security clearance and that in the circumstances known to him or her it was unjustifiable to take that risk.

---

11 Attorney-General's Department, *Submission 6.1*, p. 24.

Schedule 4 – Telecommunications interception

10.19 Schedule 4 amends the *Telecommunications (Interception and Access) Act 1979* (TIA Act) to enable 'enforcement agencies' (the Australian Federal Police, the Australian Commission for Law Enforcement Integrity and the Australian Criminal Intelligence Commission) to apply to an issuing authority for a telecommunications interception warrant for the purpose of investigating a number of the Bill's proposed offences. Currently, enforcement agencies may apply for a warrant to intercept communications for the purposes of investigating a 'serious offence', defined in the TIA Act to include any offence punishable by at least seven years imprisonment, and a list of other prescribed offences.[12]

10.21 The Bill proposes enabling these agencies to acquire a warrant to investigate all of the Bill's proposed offences. All offences in the following divisions will be defined as 'serious offences' for the purposes of the TIA Act:

- Division 82 (Sabotage)
- Division 83 (Other threats to security)
- Division 91 (Espionage)
- Division 92 (Foreign interference)
- Division 92A (Theft of trade secrets involving foreign government principal)
- Division 122 (Secrecy) and;
- Section 137.1A (aggravated offence of providing misleading information) of the *Criminal Code*.[13]

10.22 The Explanatory Memorandum provides that the purpose of the amendment is to ensure that 'law enforcement agencies have access to telecommunications interception powers to investigate these serious offences.'[14] The Explanatory Memorandum states that these powers are an 'essential tool for investigating offences involving foreign principals or communication of sensitive information'.[15]

---

12 *Telecommunications (Interception and Access) Act 1979*, section 5D.

13 National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017, sch. 4.

14 Explanatory Memorandum, p. 7.

15 Explanatory Memorandum, p. 298.

10.23 The majority of these offences are proposed to carry a maximum penalty of seven years imprisonment or more, and would accordingly fall within the current TIA Act definition of a 'serious offence', with the following exceptions:

- the aggravated offence for giving false or misleading information (section 137.1A) which is proposed to carry a maximum penalty of five years imprisonment; and
- a number of the new secrecy offences which are proposed to carry maximum penalties of between two and five years' imprisonment.

Application to aggravated offence of providing misleading information and secrecy offences

10.24 The Bill proposes the extension of telecommunications interception powers to investigations concerning the proposed section 137.1A 'aggravated offence for giving false or misleading information'.[16]

10.25 The Law Council of Australia did not support this amendment. It noted that this offence, as proposed, does not require the false or misleading information to have a nexus to a foreign country or foreign principal. Accordingly, a warrant could be obtained to investigate matters that do not pose a threat to Australia's national security. In this context, it considered the proposed expansion 'would be considerable and does not appear justified'.[17]

10.26 In response, the Attorney-General's Department submitted:

> The use of telecommunications interception powers are likely to be critical in understanding a person's intentions, associations or other prejudicial activity, as well as the person's associations, in the context of the provision of false or misleading information as part of a security clearance process.[18]

10.27 The Bill will also enable law enforcement agencies to seek warrants to investigate all secrecy offences, including:

---

16 National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017, sch. 4, cl. 2.

17 Law Council of Australia, *Submission 5*, p. 73.

18 Attorney-General's Department, *Submission 6.1*, p. 24.

- the 'inherently harmful information' offences set out in proposed section 122.1(2)-(4), which are proposed to carry a maximum penalty of five years imprisonment;
- the 'conduct causing harm to Australia's interests' offences set out in proposed section 122.2(2)-(4) , which are proposed to carry a maximum penalty of five years imprisonment; and
- unauthorised disclosure of information by a current or former Commonwealth officer, subject to a maximum penalty of two years imprisonment (proposed section 122.4).

10.28 The Statement of Compatibility with Human Rights in the Explanatory Memorandum acknowledges that telecommunications interception imposes a limitation on the right to privacy. The limitation is justified by reference to:

> 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.[19]

10.29 Mr Timothy Pilgrim, the Australian Information Commissioner and the Australian Privacy Commissioner, submitted that, consistent with Article 17 of the *International Covenant on Civil and Political Rights* (ICCPR), proposals to limit privacy protections should be demonstrably reasonable, necessary and proportionate, having regarding to the proposal's policy objectives.[20] Article 17 provides:

> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> 2. Everyone has the right to the protection of the law against such interference or attacks.[21]

---

19 Explanatory Memorandum, p. 19.

20 Office of the Australian Information Commissioner, *Submission 16*, p. 3.

21 International Covenant on Civil and Political Rights, Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966, entry into force 23 March 1976, in accordance with Article 49.

10.30 The Commissioner noted that the Bill's proposal to extend telecommunications powers to capture the expanded secrecy offences and proposed aggravated offence would increase the circumstances where personal information may be collected, accessed and disclosed under the TIA Act.[22] He raised concerns that the Explanatory Memorandum focuses on the limitation to the right to privacy in the context of espionage and foreign interference, but does not make clear the need for expanding the regime in the TIA Act to include the secrecy provisions and the aggravated offence for false or misleading information.[23]

10.31 Accordingly, the Commissioner recommended that additional information be included in the Explanatory Memorandum to explain 'how the expanded definition of 'serious offence' is reasonable, necessary and proportionate, given the likely impact of this expanded definition on individuals' privacy'.[24]

10.32 Responding to the Commissioner's concern, the Attorney-General's Department submitted that:

> The department's view is that the inclusion of secrecy offences and aggravated false and misleading information offence in the definition of serious offence under the TIA Act is reasonable, necessary and proportionate.[25]

10.33 The Department referred to the 'detailed justification' provided elsewhere in the Explanatory Memorandum for the inclusion of all of the relevant offences in the TIA Act definition of 'serious offence'.[26]

10.34 The Centre for Media Transition raised concerns that defining a 'serious offence' to include all of the proposed secrecy offences would facilitate access by agencies to information concerning journalists' sources, without adequate public interest protections.[27]

Committee Comment

10.35 The Committee has previously noted the dual objectives of the TIA Act to protect the privacy of communications by prohibiting unlawful interception,

---

22 Office of the Australian Information Commissioner, *Submission 16*, p. 3.

23 Office of the Australian Information Commissioner, *Submission 16*, p. 4

24 Office of the Australian Information Commissioner, *Submission 16*, p. 2.

25 Attorney-Generals' Department, *Submission 6.1*, p. 40.

26 Attorney-Generals' Department, *Submission 6.1*, p. 40.

27 University of Technology Sydney Centre for Media Transition, *Submission 23*, p. 5

while enabling limited interception access for the investigation of serious crime and threats to national security.[28]

10.36 The Committee considers that it is appropriate that law enforcement agencies be enabled, subject to the safeguards in the TIA Act, to investigate the offences proposed in the Bill. This includes the proposed new offences for foreign interference and theft of trade secrets, as well as the range of other serious offences that will be amended by the Bill. The Committee particularly notes the important role that telecommunications interception could play in investigating the proposed new and amended secrecy offences. Accordingly, the Committee supports these amendments.

10.37 The Committee notes that a justification for the expanded telecommunications interception laws is provided in the Explanatory Memorandum,[29] but such an explanation is absent from the Bill's *Statement of Compatibility with Human Rights*. The Statement justifies limiting the right to privacy by reference to the threat posed by espionage, foreign interference and related activities.[30] As described earlier, this offence has a broader application than information concerning espionage and foreign interference.

10.38 In recognition of concerns expressed by the Privacy Commissioner, the Committee recommends amending the Bill's *Statement of Compatibility with Human Rights* to address the matters raised by the Commissioner.[31]

Recommendation 52

10.39 The Committee recommends that the Explanatory Memorandum be amended so that the Statement of Compatibility with Human Rights explicitly addresses the necessity, reasonableness, and proportionality of the expansion of telecommunications interceptions powers to all of the offences specified in Schedule 4 of the Bill.

---

28 Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, May 2013, p. 13.

29 Explanatory Memorandum, p. 300.

30 Explanatory Memorandum, p. 19 .

31 *Human Rights (Parliamentary Scrutiny) Act 2011*, section 8.

Schedule 5 – The Foreign Influence Transparency Scheme Bill 2017

10.40 The Foreign Influence Transparency Scheme Bill 2017 (FITS Bill) proposes to establish a Foreign Influence Transparency Scheme (the Scheme). The Scheme will require persons or entities who engage in certain activities on behalf of a foreign principal to register.

10.41 On the same day that the Prime Minister introduced this Bill and the FITS Bill into the House of Representatives, the Minister for Finance introduced the Electoral Legislation Amendment (Electoral Funding and Disclosure Reform) Bill 2017 (Electoral Bill) into the Senate.

10.42 Part 1 of Schedule 5 makes amendments to the requirement to register under section 16 of the Foreign Influence Transparency Scheme Act (if, and once, it is passed). Section 16 requires a person to apply to the Secretary for registration under the scheme within 14 days of becoming liable to register. The effects of the amendments are that

> if a registrable arrangement is in existence between a person and a foreign principal at the time of the commencement of the Foreign Influence Transparency Scheme Act, the person is not required to register under the scheme before six months after the day on which that Act commences. The effect of this item is that the person must apply to the Secretary for registration within 14 days after the end of the six month period.[32]

10.43 Part 2 of Schedule 5 will amend the FITS Bill if and once the FITS Bill and the Electoral Bill have been passed by the Parliament. Schedule 5 will not take effect unless both the FITS Bill and Electoral Bills are passed.

10.44 The proposed amendments will:

- align the disclosure threshold for donor activity under the Scheme with the disclosure threshold in the Commonwealth Electoral Act ($13 500), and
- import the term 'political campaigners' into the Scheme so that:
  - lobbying a political campaigner could be a registrable activity, and
  - influencing processes in relation to a political campaigner could be a registrable activity.

---

32 Explanatory Memorandum, p. 302.

10.45 The reason amendments to the FITS Bill are contained in the Bill are explained in the Explanatory Memorandum as follows:

> The usual practice is to not have amending Schedules at the ends of Bill that establish new Principal Acts. In accordance with this practice, Schedule 5 has been included in this amending Bill rather than as a schedule to the Foreign Influence Transparency Scheme Bill 2017.[33]

10.46 The Joint Standing Committee on Electoral Matters (JSCEM) tabled its advisory report on the Electoral Bill on 9 April 2018. A key recommendation in the JSCEM report was that instead of the categories of 'third party campaigner' and 'political campaigner' being established as registration thresholds, the Government consider establishing a publicly available 'Transparency Register' for all entities involved in 'political expenditure', with mandatory registration for activities that reach a minimum 'expenditure threshold'. JSCEM considered that, due to its common usage, the term 'disclosure threshold' should not be used.[34]

Committee comment

10.47 The Committee notes that Schedule 5 to the Bill proposes amendments to the Foreign Influence Transparency Scheme Bill 2017 (FITS Bill) that will only come into effect if, and once, that Bill is passed. The Committee is reporting on its review of the FITS Bill separately.

10.48 In addition to the FITS Bill, some of the amendments in Schedule 5 will only come into effect following the passage of the Electoral Legislation Amendment (Electoral Funding and Disclosure Reform) Bill 2017 (Electoral Bill). The JSCEM has recently tabled its report on the Electoral Bill and the Committee recognises that, if JSCEM's recommendations are accepted by the Government, then certain consequential amendments to Schedule 5 are likely to also be required.

---

33 Explanatory Memorandum, p. 302.

34 Joint Standing Committee on Electoral Matters, *Advisory Report on the Electoral Legislation Amendment (Electoral Funding and Disclosure Reform) Bill 2017*, April 2018, pp. 29–30.

Consequential amendments

Cessation of citizenship

10.49 Schedule 1 to the Bill includes consequential amendments to section 35A of the *Australian Citizenship Act 2007*. Section 35A of the *Australian Citizenship Act 2007* was introduced in 2015 to enable the Minister to determine that a dual-citizen has ceased to be an Australian citizen where:

- the person has been convicted of specified offences, including treason, treachery, espionage or sabotage,[35]
- the person has been sentenced to a period of imprisonment of at least six years, or to periods of imprisonment that total at least six years,[36] and
- the Minister is satisfied of certain other prescribed criteria.[37]

10.50 The Committee reviewed the proposed introduction of section 35A through its review of the Australian Citizenship Amendments (Allegiance to Australia) Bill 2015. In its advisory report, the Committee acknowledged significant concerns raised by various stakeholders, both in relation to section 35A and the amendments more broadly. The Committee noted its support for

> the policy intention of the [Australian Citizenship Amendments (Allegiance to Australia) Bill 2015] to help protect the community from person who have clearly renounced their allegiance to Australia by engaging in serious terrorism-related acts that harm Australian or Australian interests.[38]

10.51 In relation to section 35A, the Committee stated:

---

35 *Australian Citizenship Act 2007*, section 35A(1)(a)(ii) and (v).

36 *Australian Citizenship Act 2007*, section 35A(1)b).

37 *Australian Citizenship Act 2007*, section 35A. The criteria includes that the person has been sentenced to a period of imprisonment of at least six years and that the Minister is satisfied that the conviction demonstrates that the person has repudiated their allegiance to Australia. The Minister must also consider the public interest in the person remaining in retaining their citizenship, including the severity of the conduct, the threat posed by the person, the person's age (and if under 18, the best interests of the child), the person's connection to the other country to which they are a citizen or national, Australia's international relations and any other matters of public interest (section 35A(1)(e)).

38 Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Australian Citizenship Amendment (Allegiance to Australia) Bill 2015,*

> The Committee considers that revocation of citizenship under proposed section 35A should only follow appropriately serious conduct that demonstrates a breach of allegiance to Australia. This is consistent with the intent of the Bill … the Committee considers that the provision should more appropriately target the most serious conduct that is closely linked to a terrorist threat.[39]

10.52 In keeping with these statements, the majority of provisions in the Bill which gained Committee support concerned terrorism related conduct. However, the Committee supported the inclusion of a small number of non-terrorism related offences in section 35A: treason, espionage, sabotage and treachery.

10.53 Following the Committee's review, the Bill's Revised Explanatory Memorandum stated:

> The specified offences in 35A(1)(a) reflect the policy intention that an offence listed for the purpose of cessation under new subsection 35A(1) must be a terrorism-related offence where the maximum penalty is at least 10 years imprisonment. The offences are of a nature that on the face of them a person who undertakes such offences has repudiated their allegiance to Australia.[40]

> The purpose of new section 35A is to deal with the threat caused by those who have acted in a manner contrary to their allegiance to Australia by removing them from formal membership of the Australian community. Cessation of citizenship is a very serious outcome of very serious conduct that demonstrates a person has repudiated their allegiance to Australia (refer to paragraph 35A(1)(d)). Removing a person's formal membership of the Australian community is appropriate to reduce the possibility of a person engaging in acts or further acts that harm Australians or Australian interests.[41]

Proposed expansion of citizenship cessation regime

10.54 The Bill proposes substituting the references to the current treachery, espionage and sabotage offences, which will be repealed, for the new versions of these offences proposed by the Bill.[42]

---

39 Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Australian Citizenship Amendment (Allegiance to Australia) Bill 2015*, pp. 114-115.

40 Revised Explanatory Memorandum, p. 31.

41 Revised Explanatory Memorandum, p. 33.

42 Schedule 1, items 29-30.

10.55 The Committee questioned whether the application of section 35A of the *Australian Citizenship Act 2007* to all of the proposed new sabotage and espionage offences was intentional and, if so, whether this could be addressed in the Explanatory Memorandum. The Attorney-General's Department confirmed that this would be the effect, and that 'the Explanatory Memorandum could more explicitly state that this effect was intended if the Committee would consider this useful'.[43]

10.56 In response to another question, about why these amendments applied to all sabotage and espionage offences, and whether the Minister could be given a discretionary power to approve a citizenship application where an applicant had been convicted of one of the less serious sabotage or espionage offences, the Department advised:

> The scope of espionage and sabotage offences is a matter for the Parliament. The policy intention of the consequential amendments to the Australian Citizenship Act is to ensure that the scope of section 35A of the Australian Citizenship Act aligns with the scope of the enacted offences, as determined by the Parliament.[44]

Committee Comment

10.57 The Committee has considered the Bill's treachery, sabotage and espionage offences earlier in this report (see Chapters 6, 8 and 9), and notes that the amendments proposed in the Bill will broaden the scope of the equivalent existing offences. Accordingly, the Bill's consequential amendments to section 35A of the *Australian Citizenship Act 2007* will have the effect of broadening the range of conduct that will expose a dual citizen to the possibility of losing his or her Australian citizenship.

10.58 The Committee recognises the serious consequences which flow from removing a person's formal membership of the Australian community. Accordingly, the Committee notes its previous comment that citizenship laws should target the 'most serious conduct that is closely linked to a terrorist threat'.[45]

---

43 Attorney-General's Department, *Submission 6.1*, p. 90.

44 Attorney-General's Department, *Submission 6.1*, p. 90.

45 Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Australian Citizenship Amendment (Allegiance to Australia) Bill 2015*, September 2015, p. 115.

10.59 It is the Committee's view that a strong justification for any expansion of the existing citizenship loss laws is required. In response to a question from the Committee, the Attorney-General's Department advised:

> The policy intention of the consequential amendments to the Australian Citizenship Act is to ensure that the scope of section 35A of the Australian Citizenship Act aligns with the scope of the enacted offences, as determined by the Parliament.[46]

10.60 The Committee also notes its previous recommendation that section 35A should be limited to offences that carry a maximum penalty of at least 10 years imprisonment.[47] Under the current Bill, a conviction for the offence of 'preparing for or planning sabotage offence' (proposed section 82.9) is punishable by a maximum penalty of imprisonment for seven years.[48] Accordingly, the Committee considers this offence should not be included within the scope of section 35A.

10.61 The Committee considers that section 35A should apply to serious national security offences. This should include the reformed treason, treachery, espionage and sabotage offences, as well as the new foreign interference offences. However, the Committee considers that section 35A should not apply to:

- proposed section 82.9, given its lower maximum penalty, consistent with the Committee's previous views,
- section 83.4 (interference with political rights and duties) as, notwithstanding that interfering with political rights and duties is a very serious matter warranting criminal sanctions, it is not inherently a matter of national security, and
- the proposed new secrecy offences in Part 5.6 as, notwithstanding that many aspects of these offences plainly relate to national security, it will not always be the case that a person committing a secrecy offence endangers national security.

---

46 Attorney-General's Department, *Submission 6.1*, p. 90.

47 Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Australian Citizenship Amendment (Allegiance to Australia) Bill 2015*, September 2015, p. 115.

48 Proposed section 82.9.

Recommendation 53

10.62 The Committee recommends that Schedule 1, item 29 of the Bill be amended such that section 35A of the *Australia Citizenship Act 2007* applies to the foreign interference offences in the Bill, and does not apply to

- **proposed section 82.9 (preparing for or planning sabotage offence),**
- **proposed section 83.4 (interference with political rights and duties), or**
- **proposed Part 5.6 – Secrecy of information.**

Citizenship applications

10.63 Schedules 1 and 2 to the Bill also contain amendments to the definition of 'national security offence' in section 3 of the *Australian Citizenship Act 2007*, which affects the treatment of applications for Australian citizenship made by persons who are not a national or citizen of any country ('stateless persons').

10.64 Currently, the Minister is obliged to refuse certain citizenship applications made by stateless persons, where the applicant has been convicted of a 'national security offence' including:

- treachery,
- sabotage,
- inciting mutiny,
- assisting prisoners of war to escape,
- unlawful drilling,
- interfering with political liberty,
- espionage, or
- an 'official secrets' offence.[49]

10.65 The Bill proposes to repeal these offences and substitute with new versions of the offences, including:

---

[49] *Australian Citizenship Act 2007*, sections 17(4A); 19D(6); 24(4A); and 30(5). Refer to the definition of a 'national security offence' in section 3 of the Act.

- the proposed offences to be inserted into Part 5.1 of the *Criminal Code*, such as the introducing vulnerability offences in Division 82, and the proposed new espionage offences in Division 91, and
- the proposed new secrecy offences in Part 5.6.[50]

10.66 Currently, the Crimes Act offence of destroying or damaging Commonwealth property is a national security offence. The Bill does not propose listing the new version of this offence, which is proposed to be inserted into Part 7.2 of the *Criminal Code*, as a national security offence.

10.67 The Committee asked the Department why the amendments include all of the proposed new offences in Division 82 (sabotage) and Division 91 (espionage), rather than being limited to the most serious of the offences. The Committee also asked whether, if this was intended, the Minister could possess a discretion to approve a citizenship application where the applicant has been convicted of one of the less serious sabotage or espionage offences. The Attorney-General's Department responded:

> The scope of espionage and sabotage offences is a matter for the Parliament. The policy intention of the consequential amendments to the *Australian Citizenship Act* is to ensure that the scope of the definition of 'national security offence' in the *Australian Citizenship Act* aligns with the scope of the enacted offences, as determined by the Parliament.
>
> This would mean that the Minister could consider any of the sabotage or espionage offences in proposed new Divisions 82 and 91 of the *Criminal Code* when exercising a power in the Australian Citizenship Act that relies on the definition of 'national security' in section 3 of that Act.[51]

International obligations to prevent statelessness

10.68 Australia is party to the *Convention on the Reduction of Statelessness*, which imposes obligations directed at reducing the incidence of statelessness, including obligations related to the conferral and withdrawal of citizenship. The Introductory Note to the Convention records that:

---

50 Schedule 1, item 28; Schedule 2, item 11.

51 Attorney-General's Department, *Submission 6.2*, p. 6.

> By setting out rules to limit the occurrence of statelessness, the Convention gives effect to article 15 of the Universal Declaration of Human Rights which recognizes that 'everyone has the right to a nationality'.[52]

10.69 The Attorney-General's Department submitted that the obligations set out in the *Convention on the Reduction of Statelessness*:

> … are relevant to the Bill to the extent that the Bill makes changes to offences in the *Criminal Code* and *Crimes Act* for which a conviction may, under the *Australian Citizenship Act 2007 (Cth)*, operate as a bar to the grant of citizenship or as a ground for cessation of citizenship.[53]

10.70 In response to the Committee's queries, the Attorney-General's Department advised that further consideration would be given to the interaction between the Bill and Australia's obligations under the 1961 Reduction Convention.[54] The Department subsequently advised that:

> We have considered this issue further, and our view is that some changes may be needed to remove a small number of offences in the [B]ill from the scope of the definition of 'national security offences' in the Australian Citizenship Act, and we are working through those details with the Department of Home [A]ffairs, which administers the Australian Citizenship Act.[55]

Committee Comment

10.71 As discussed in Chapter 1, the Committee has reviewed the Bill with a view to ensuring that each measure is clear and unambiguous in its terms; enforceable; proportional and appropriately targeted to the threat.

10.72 The Committee has considered the Bill's treachery, sabotage and espionage offences earlier in this report (see Chapters 6, 8 and 9), and notes that the amendments proposed in the Bill will broaden the scope of the equivalent existing offences. Accordingly, the Bill's proposed amendments to the definition of 'national security offence 'in the *Australian Citizenship Act 2007* will have the effect of broadening the range of conduct that will mandate the refusal of an application for citizenship by a stateless person. The Committee

---

52 1961 Convention on the Reduction of Statelessness: Introductory note by the Office of the United Nations High Commissioner for Refugees.

53 Attorney-General's Department, *Submission 6.1,* pp. 90–91.

54 Attorney-General's Department, *Submission 6.1,* p. 91.

55 Ms Anna Harmer, First Assistant Secretary, Attorney-General's Department, *Committee Hansard*, Melbourne, 16 March 2018, p. 36.

recognises that a number of these provisions do not have a clear nexus to national security.

10.73 The Committee notes the Attorney-General's Department's advice that further amendments to these provisions will be forthcoming in relation to Australia's obligations under the *Convention on the Reduction of Statelessness*. At the time of drafting, these amendments had not been made available to the Committee for its consideration. The Committee considers that in order for these measures to be proportional and appropriately targeted to the threat, their operation should be limited to convictions for offences with a clear national security nexus.

Recommendation 54

10.74 The Committee recommends that the Bill be amended such that the phrase 'national security offence' in the *Australian Citizenship Act 2007* is limited to those offences which contain a clear nexus to national security.

Recommendation 55

10.75 The Committee recommends that the Explanatory Memorandum be amended so that the Statement of Compatibility with Human Rights explicitly addresses the interaction between the proposed consequential amendments to citizenship application provisions, and Australia's international obligations regarding stateless persons.

Deportation

10.76 Consequential amendments in Schedule 1 also affect the Minister's powers of deportation in Division 9 of the *Migration Act 1958*. This regime enables the Minister to order the deportation of a non-citizen who

- has resided in Australia for less than ten years, and has been convicted of an offence punishable by at least one year of imprisonment,[56] or
- has resided in Australia for any period of time and:
  - has been convicted of 'certain serious offences',[57] or
  - is the subject of an ASIO adverse security assessment.[58]

56 *Migration Act 1958*, section 201.

57 *Migration Act 1958*, section 203.

58 *Migration Act 1958*, section 202.

10.77 Currently, the list of 'certain serious offences' includes treason, treachery, sabotage, inciting mutiny; and assisting prisoners of war to escape.[59] The Bill proposes amending section 203 of the *Migration Act 1958* to replace these offences with the modernised versions of these offences proposed by the Bill.[60] This will include the new proposed sabotage and introducing vulnerability offences in Division 82 of the *Criminal Code*. The Attorney-General's Department submitted that it 'considers all of the sabotage offences in Division 82 to be serious, as reflected in the maximum penalties applied to the offences'.[61]

Committee Comment

10.78 The Committee has considered the Bill's sabotage, treachery and advocating mutiny offences earlier in this report (see Chapters 8 and 9), and notes that the amendments proposed in the Bill will broaden the scope of the equivalent existing offences. Accordingly, the Bill's proposed amendments to the list of 'certain serious offences' in section 203 of the *Migration Act 1958* will have the effect of broadening the range of circumstances in which the Minister may order the deportation of a non-citizen who has resided in Australia for more than ten years.

10.79 However, the Committee notes that the conduct captured by the broadened offences proposed in the Bill is potentially very serious. Further, the Committee recognises that—apart from conviction for 'certain serious offences'—there are a number of other avenues available to the Minister to order the deportation of such persons. These include the 'character test' in section 501 of the *Migration Act* and ASIO's ability to issue an adverse security assessment if the person poses an unacceptable risk to security. As such, the Committee does not consider the broadening of section 203 of the *Migration Act 1958* to cover the amended offences unreasonable or out of step with existing provisions.

Presumption against bail

10.80 Consequential amendments in Schedule 1 to the Bill affect laws relating to the presumption against bail contained in section 15AA of the *Crimes Act 1914*.

---

59 *Crimes Act 1914*, sections 24AA, 24AB, 25 and 26.

60 Schedule 1, item 47–48.

61 Attorney-General's Department, *Submission 6.1*, p. 85.

10.81 State and territory courts hear and deal with federal offence bail applications according to their own bail procedures and laws.[62] These laws routinely require judicial officers to consider a range of factors when determining the appropriateness of the grant of bail, including the seriousness of the offence; the likelihood that the accused would fail to appear; and the possibility the accused could interfere with witnesses or evidence.[63]

10.82 The Explanatory Memorandum notes that most state and territory criminal procedure laws provide for a general presumption in favour of bail, which ensures that deprivations of liberty are kept to a minimum by allowing the temporary release of the accused person pending criminal proceedings.[64] This presumption is consistent with article 9(3) of the *International Covenant on Civil and Political Rights* (ICCPR), which provides:

> It shall not be the general rule that persons awaiting trial shall be detained in custody…

10.83 However, the Explanatory Memorandum states that the general presumption in favour of bail may be displaced in certain circumstances:

> The presumption against bail is appropriately reserved for serious offences recognising the need to balance the right to liberty and the protection of the community.[65]

10.84 The Bill will impose a presumption against bail upon a number of the new and modified offences proposed by the Bill.[66] Bail will only be granted for these offences where the accused can demonstrate exceptional circumstances exist to justify bail.

10.85 Currently, section 15AA of the Crimes Act imposes a presumption against Bail for a number of national security offences including offences against Subdivision C of Division 80 of the *Criminal Code* (urging violence and advocating terrorism or genocide); Division 91 of the *Criminal Code* (espionage); and section 24AA (treachery) of the Crimes Act.

---

62 *Judiciary Act 1903, section* 68.

63 For example, *Bail Act 2013 (NSW), Bail Act 1980 (QLD).*

64 Explanatory Memorandum, p. 13 .

65 Explanatory Memorandum, p. 13.

66 Schedule 1, items 38 and 39.

10.86 The presumption's application to these offences is limited to circumstances where it is alleged that the conduct caused, or carried a substantial risk of causing the death of a person. In these circumstances, bail cannot be granted unless exceptional circumstances exist to justify bail.[67]

10.87 The Bill proposes amending section 15AA to extend the presumption against bail to:

- Division 80 offences, not only those offences in Subdivision C. This will have the effect of continuing to limit bail for treachery offences, and creating a new limitation on bail for treason offences,
- the proposed new espionage offences in Division 91, and
- new proposed offences of intentional foreign interference (section 92.2(1)) and reckless foreign interference (section 92.3(1)).

10.88 Consistent with current requirements, the Bill proposes that a person charged with, or convicted of a Division 80 or Division 91 offence will not be granted bail where it is alleged that their conduct caused, or carried a substantial risk of causing the death of a person, unless exceptional circumstances exist to justify the grant of bail.[68]

10.89 In contrast, the Bill proposes that the foreign interference offences will attract the presumption against bail wherever 'it is alleged that any part of the conduct the defendant engaged in involved making a threat to cause serious harm or a demand with menaces'.[69] The proposed amendment does not require that the conduct caused, or carried a substantial risk of causing death.

10.90 The Explanatory Memorandum states that extending the presumption against bail to the new foreign interference offences

> … is appropriate given that the conduct is similar in nature to that of an espionage offence. However, it is appropriate that a person being prosecuted for a foreign interference offence against section 92.2(1) and 92.3(1) should only be subject to a presumption against bail in circumstances when there is a threat of harm.[70]

---

67 *Crimes Act 1914*, section 15AA.

68 *Crimes Act 1914*, proposed subsections 15AA(2)(c) and (d).

69 *Crimes Act 1914*, proposed section 15AA(2)(e).

70 Explanatory Memorandum, p. 216.

10.91 The Law Council of Australia noted that it opposes in principle laws that create a presumption against bail, on the basis that such laws are inconsistent with the presumption of innocence.[71] Accordingly, the Law Council did not support the proposed amendments to section 15AA. In reference to Article 9(3) ICCPR, the Law Council submitted:

> The United Nations Human Rights Committee has stated on a number of occasions that pre-trial detention should remain the exception and that bail should be granted except in circumstances where the likelihood exists that, for example, the accused would abscond, tamper with evidence, influence witnesses or flee from the jurisdiction.[72]

10.92 The Law Council advocates for the presumption in favour of bail to operate in all cases.[73] In relation to the particular offences proposed to be subject to a presumption against bail, the Council raised concerns that

- given the potential complexity of any trial for an espionage, treason and foreign interference offence, the period of pre-trial detention may be lengthy, and
- due to the breadth of the proposed offences, relatively innocuous or trifling conduct could be captured.[74]

10.93 In the event that the proposed presumption against bail is to proceed, the Law Council recommended:

- the Independent National Security Legislation Monitor should review the bail provisions in section 15AA of the Crimes Act, including the provision's impact on children; and
- there should be no provision for a grant of bail to be stayed if the prosecution notifies an intention to appeal.[75]

10.94 The Attorney-General's Department did not agree with the Law Council's submission, noting that the offences proposed to be subject to a presumption against bail are 'very serious offences'.[76]

---

71 Law Council of Australia, *Submission 5*, p. 74 .

72 Law Council of Australia, *Submission 5*, p. 75, referring to the UN Human Rights Committee, *Smantser v Belarus* (1178/03); *WBE v the Netherlands* (432/90); *Hill and Hill v Spain* (526/93).

73 Law Council of Australia, *Policy Statement on Principles Applying to Detention in a Criminal Law Context*, 22 June 2013, p. 5.

74 Law Council of Australia, *Submission 5*, p. 74.

75 Law Council of Australia, *Submission 5*, p. 78.

10.95 Regarding the thresholds for treason, treachery and espionage offences (causing death or a risk of death); compared to the threshold for foreign interference offences (threat or menaces), the Attorney-General's Department submitted that the latter

> recognises the significant consequences for an individual's personal safety and mental health if the conduct involves serious harm (consistent with the definition of 'serious harm' in the Dictionary to the Criminal Code) or making a demand with menaces' (as defined in section 138.2 of the Criminal Code).[77]

Committee comment

10.96 The Committee notes that section 15AA of the Crimes Act operates to

- impose a presumption against bail that allows bail only in exceptional circumstances, and
- even where exceptional circumstances exist, allows the detention of a successful bail applicant for up to three days pending a prosecutor's appeal.[78]

10.97 The Committee considers that laws that create a presumption against bail should be limited to only the most serious offences.

10.98 The Committee considers that treason, treachery and espionage offences that cause, or could cause the death of a person, possess this quality. The Committee therefore supports the continued the application of section 15AA to the revised treachery and espionage offences. The Committee also supports the proposal to extend the operation of section 15AA of the Crimes Act to include treason offences. The Committee notes that the deprivation of the accused's liberty for these offences will be limited to cases where the conduct caused the death of a person, or carried a substantial risk of this occurring.[79]

10.99 The Committee also supports applying a presumption against bail to the foreign interference offences in proposed sections 92.2(1) and 92.3(1). However, the Committee recommends that the circumstances in which this presumption arises should be consistent with the threshold for treason,

---

[76] Attorney-General's Department, *Submission 6.1*, p. 25.

[77] Attorney-General's Department, *Submission 6.2*, p. 3.

[78] *Crimes Act 1914*, section 15AA(3C) and (3D).

[79] *Crimes Act 1914*, section 15AA(2)(c).

treachery and espionage offences. The Committee notes the amendments in the Bill currently apply to a foreign interference offences founded on a 'demand with menaces'. This is a considerably lower threshold than that applied to treachery and espionage offences (death, or risk of death).

10.100 The Committee considers that thresholds for a presumption against bail should be high and should be consistent. Accordingly, the presumption against bail should apply to section 92.2(1) or 92.3(1) only where the death of a person is alleged to have been caused by conduct that is a physical element of the offence; or conduct that is a physical element of the offence that carried a substantial risk of causing the death of a person.

10.101 The Committee notes that section 15AA of the Crimes Act has a broader operation than the amendments currently before the Committee. The Law Council of Australia has raised general concerns about the operation of section 15AA, including:

- subsection 15AA(3D), which has the effect of enabling the detention for up to three days, of any person charged with an offence meeting the criteria set out in section 15AA, regardless of their personal circumstances, and
- the impact of section 15AA on children.[80]

10.102 The Committee supports consideration of these provisions by the Independent National Security Legislation Monitor (INSLM), and notes that the INSLM is currently conducting a *review into the prosecution and sentencing of children for Commonwealth terrorist offences*, following a reference by the Prime Minister.[81]

Recommendation 56

10.103 The Committee recommends that the Bill be amended to provide that section 15AA(1) of the *Crimes Act 1914* applies to an offence against proposed Division 80, Division 91, and Division 92 of the *Criminal Code* only if:

---

80 Law Council of Australia, *Submission 5*, pp. 74–76.

81 Independent National Security Legislation Monitor, 'Review: the prosecution and sentencing of children for Commonwealth terrorist offences', < http://www.inslm.gov.au/current-review-work> viewed 11 May 2018.

- **the death of a person is alleged to have been caused by conduct that is a physical element of the offence, or**

- **conduct that is a physical element of the offence carried a substantial risk of causing the death of a person.**

In-camera proceedings

10.104 The power to conduct proceedings in-camera is set out in section 93.2 of the *Criminal Code*. The provision applies to any proceeding heard in a federal court, territory court, or court exercising federal jurisdiction, and is not limited to proceedings under Part 5.2 of the *Criminal Code*.[82] The section enables a judicial officer to order, or make directions to:

- exclude the public, or certain persons from all or part of the proceedings,
- issue a non-publication order, which would prevent the publication of a report of the whole, or a specified part of the proceedings, and/or
- restrict access to the Court file or any part of it, for example, an affidavit, or exhibit.

10.105 Currently, the Court may make such orders where it is in the interest of the 'security or defence' of the Commonwealth. For the purposes of this section, the *Criminal Code* provides that the

> 'security or defence' of a country includes the operations, capabilities and technologies of, and methods and sources used by, the country's intelligence or security agencies.[83]

10.106 The Bill proposes enabling such orders to be made in circumstances where it is in the 'interest of Australia's national security'. The Bill proposes defining national security to include a country's

- defence,
- protection of its border from serious threats,
- protection from espionage, sabotage, terrorism, foreign interference and political violence, and
- political, military or economic relations with another country or other countries.[84]

---

82 This point was clarified by the Attorney-General's Department in *Submission 6.5*, p. 4.

83 *Criminal Code*, section 90.1.

84 Proposed section 90.4.

10.107 As discussed in Chapter 3, aspects of the Bill's definition of 'national security' are intended to align with the *National Security Information (Criminal and Civil Proceedings) Act 2004* (the NSI Act), which 'substantially implemented' the ALRC's 2004 recommendations in *Keeping Secrets: The Protection of Classified and Security Sensitive Information*.[85] Similarly to section 93.2, the object of the NSI Act is to prevent the disclosure of information in federal criminal proceedings and civil proceedings where the disclosure is likely to prejudice national security.[86]

10.108 The ALRC also recommended in its 2004 report that section 93.2 of the *Criminal Code* be repealed with the introduction of the NSI Act.[87] Despite this, the Attorney-General's Department considered that there was 'significant value' in section 93.2 being retained.

> The NSI Act neither excludes nor impedes a court's other powers, including powers to make other protective orders such as closure of court and non-publication orders, and sections 20B and 38AB of the NSI Act refer expressly to section 93.2 of the Criminal Code.
>
> The NSI Act provides a comprehensive regulatory framework for the disclosure, storage and handling of all national security information involved in federal criminal proceedings or civil proceedings, whether in documentary or oral form. The NSI Act, once invoked by the prosecutor, applies to the whole proceeding and provides a structure for a court to follow where national security information is disclosed in proceedings.
>
> … Section 93.2 allows a presiding judge to make whatever orders are considered appropriate in the interests of the security or defence of the Commonwealth in a more targeted way where the varied protective options available under the NSI Act are not required.[88]

10.109 The Attorney-General's Department noted that the proposed amendment in the Bill 'ensures the alignment of this provision with the new definitions proposed to be inserted by the Bill'.[89] It added:

---

85 Attorney-General's Department, *Submission 6.1*, pp. 2, 44.

86 *National Security Information (Criminal and Civil Proceedings) Act 2004*, section 3.

87 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information* (Report 98), May 2004, pp. 478, 508.

88 Attorney-General's Department, *Submission 6.5*, p. 4.

89 Attorney-General's Department, *Submission 6.1*, p. 49.

> Section 93.2 complements any available state and territory laws allowing for suppression orders or non-publication orders to be imposed on national security grounds (such the Open Courts Act 2013 (Vic) and the Court Suppression and Non-Publication Orders Act 2010 (NSW)). Section 93.2 provides a power to appropriately manage proceedings where the court is satisfied that it is in the interests of Australia's national security to do so. This is an important protection and the decision as to whether to exercise the power remains with the court.[90]

Committee Comment

10.110 While section 93.2 of the *Criminal Code* has a similar objective to the *National Security Information (Criminal and Civil Proceedings) Act 2004* (NSI Act), the Committee recognises its distinct purpose and the value that it adds.

10.111 The Committee has discussed the Bill's proposed definition of national security earlier in this report (see Chapter 3). The Committee supports the proposed amendment to align the terminology used in section 93.2 of the *Criminal Code* with the new definition of national security in the Bill.

10.112 The Committee notes the broad application of section 93.2 to all proceedings heard in a federal court, territory court, or court exercising federal jurisdiction, not only proceedings instituted for an offence against Part 5.2 of the *Criminal Code*.[91] The Committee recommends that the Explanatory Memorandum be amended to make the scope of the provision clear.

Recommendation 57

10.113 The Committee recommends that the Explanatory Memorandum for the Bill be amended to clarify the scope and application of section 93.2 of the *Criminal Code*.

Standard non-parole periods

10.114 A number of the Bill's new and modified offences will be subject to section 19AG of the Crimes Act. This section requires a sentencing Court to impose a non-parole period that is

- three-quarters of the sentence imposed by the Court, or

---

90 Attorney-General's Department, *Submission 6.1*, pp. 48–49.

91 Explanatory Memorandum, p. 204.

- where the sentence imposed by the Court is imprisonment for life, three-quarters of 30 years.

10.115 Currently, section 19AG of the Crimes Act requires minimum non-parole periods to be fixed in relation to all convictions for

- offences against section 24AA of the Crimes Act (treachery);
- terrorism offences;
- offences against Division 80 of the *Criminal Code (*treason, urging violence and advocating terrorism or genocide); and
- offences against Division 91 of the *Criminal Code* (espionage).

10.116 Section 19AG will continue to apply to the modified treachery and treason offences, and all of the proposed new espionage offences in the Bill. The proposed espionage and treachery offences are broader in scope than current offences (see Chapters 6 and 9), therefore expanding the operation of section 19AG. The Explanatory Memorandum does not comment on the effect of all of the new espionage laws, and the extended treachery offence, being subject to minimum non-parole periods.[92]

10.117 The Law Council of Australia opposes section 19AG of the Crimes Act. The Council submitted that while section 19AG does not limit a judge's discretion in imposing a head sentence, the provision removes all judicial discretion concerning the non-parole period.[93]

10.118 In its submission, the Law Council characterised provisions which impose a minimum non-parole sentence as undermining the independence of the judiciary and threatening an essential component of the rule of law.[94] The Law Council submitted that such provisions remove the ability of courts to consider relevant factors, such as the offender's criminal history, individual circumstances or whether there are any mitigating factors, such as mental illness or other forms of hardship or duress. The Law Council submitted that this can result in disproportionately harsh sentences, and that it was unlikely that judicial officers would impose a lower head sentence in order to mitigate the impact of the mandated non-parole period.[95]

---

92 Explanatory Memorandum, p. 216.

93 Law Council of Australia, *Submission 5*, p. 77.

94 Law Council of Australia, *Submission 5*, p. 77.

95 Law Council of Australia, *Submission 5*, p. 77.

10.119 At a public hearing, Mr Morry Bailes, President of the Law Council told the Committee that

> taking away judicial discretion leads to inequity and injustice. Imposing mandatory minimums of any type will ultimately lead, in some instances, to poor outcomes. The legislature is entitled to set maximum penalties … but we will always argue that there should be unfettered judicial discretion.'[96]

10.120 The Law Council recommended that:

- the mandatory minimum non-parole period for terrorism offences, Division 80 offences and Division 91 offences under section 19AG should be repealed; and (if not repealed)
- the Independent National Security Legislation Monitor should review section 19AG of the Crimes Act, including its impact on children.[97]

10.121 The Attorney-General's Department responded to the Law Council's concerns as follows:

> The Bill does not amend section 19AG other than to remove an obsolete reference to the offence of treachery which is being repealed by the Bill.[98]

10.122 The Department did not comment on the appropriateness of section 19AG applying to all of the proposed new espionage offences, or the extended treachery offence.

Committee comment

10.123 The Committee acknowledges the important role the Court plays in determining an appropriate sentence for each offender, taking into account a range of circumstances including the nature of the offence and the offender's personal circumstances. Section 19AG of the Crimes Act limits this judicial discretion. The Committee notes that while the Bill does not propose to amend section 19AG directly, the Bill will extend its operation by expanding the scope of the espionage and treachery offences that are subject to it (see Chapters 6 and 9).

---

96 Mr Morry Bailes, President, Law Council of Australia, *Committee Hansard*, Canberra, 30 January 2010, p. 54.

97 Law Council of Australia, *Submission 5*, p. 78.

98 Attorney-General's Department, *Submission 6.1*, p. 25.

10.124 It would be appropriate for the operation of section 19AG to be limited to the most serious espionage offences in the Bill. Accordingly, the Committee considers that the operation of section 19AG should be limited to:

- proposed section 91.1(1)—'dealing with information etc. concerning national security which is or will be made available to a foreign principal', with intention as to national security, and
- proposed section 91.2(1)— 'dealing with information etc. which is or will be made available to a foreign principal', with intention as to national security.

Recommendation 58

10.125 The Committee recommends that the Bill be amended to provide that section 19AG of the *Crimes Act 1914*, relating to minimum non-parole periods for certain offences, applies to an espionage offence against section 91.1(1) or 91.2(1), rather than all espionage offences in Division 91.

10.126 The Committee recognises that section 19AG has a broader operation than the proposed offences currently before the Committee, and notes the Law Council of Australia's general concerns about the provision, including its impact on children. The Committee supports consideration of this provision by the Independent National Security Legislation Monitor (INSLM), and notes that the INSLM is currently conducting a *review into the prosecution and sentencing of children for Commonwealth terrorist offences*, following a reference by the Prime Minister.[99]

[99] Independent National Security Legislation Monitor, 'Review: the prosecution and sentencing of children for Commonwealth terrorist offences', < http://www.inslm.gov.au/current-review-work> viewed 11 May 2018.

11. Concluding comments

11.1 As discussed in Chapter 1 of this report, the Committee accepts that there is a pressing need to strengthen and modernise current espionage and foreign interference laws, and supports the intent of the Bill to achieve this outcome. In doing so, the Committee recognises that the Bill proposes to re-write substantially Australia's criminal laws relating to secrecy, espionage, foreign interference and sabotage.

11.2 The Committee agrees that the secrecy provisions—and the other new or substantially broadened provisions of the Bill—should be monitored and reviewed after an appropriate period to ensure they are working as intended. To this end, the Committee recommends an independent review of the provisions after three years.

Recommendation 59

11.3 The Committee recommends that, after a period of three years, the Independent National Security Legislation Monitor be required to conduct a review of Division 82 (sabotage), Part 5.2 (espionage, foreign interference, theft of trade secrets), and Part 5.6 (secrecy) of the *Criminal Code*.

A copy of the report on the independent review should be provided to the Attorney-General, who should be required to provide it to the Committee. Any amendments proposed to be made to the laws as a result of the review should be referred to the Committee for inquiry.

11.4 The Committee also notes that there were a number of drafting errors identified during the inquiry, both in the Explanatory Memorandum and in the Bill itself. While the majority of these errors are minor, it is possible that

some could have unintended consequences. The Committee considers it essential that these errors are identified and fixed before the Bill passes through the Parliament.

Recommendation 60

11.5 The Committee recommends that the Attorney-General's Department review the Bill and Explanatory Memorandum in detail with a view to making amendments to correct any drafting errors prior to the conclusion of debate in the Parliament.

11.6 The Committee thanks the broad range of organisations and individuals who contributed to the Committee's comprehensive review of the Bill.

Mr Andrew Hastie MP
Chair
June 2018

A. List of submissions and exhibits

Submissions

1 Tony Kevin

- 1.1 Supplementary

2 Benji Wakely

3 E. Anne Lanham

4 Lucy Strang

5 Law Council of Australia

- 5.1 Supplementary
- 5.2 Supplementary

6 Attorney-General's Department

- 6.1 Supplementary
- 6.2 Supplementary
- 6.3 Supplementary
- 6.4 Supplementary
- 6.5 Supplementary

7 Australian Lawyers for Human Rights

- 7.1 Supplementary

8 Commonwealth Ombudsman

9 Joint media organisations

- 9.1 Supplementary
- 9.2 Supplementary
- 9.3 Supplementary

10 Human Rights Watch

11 Human Rights Law Centre

- 11.1 Supplementary
- 11.2 Supplementary

12 Australian Lawyers Alliance

- 12.1 Supplementary

13 Inspector-General of Intelligence and Security

- 13.1 Supplementary
- 13.2 Supplementary

14 Ms Valerie Heath

15 Mr Peter Jennings

16 Office of the Australian Information Commissioner

- 16.1 Supplementary
- 16.2 Supplementary

17 Australian Human Rights Commission

18 United Nations Special Rapporteur on the right to privacy

19 Dr Lawrence McNamara

20 Clive Hamilton and Alex Joske

21 International Committee of the Red Cross and Australian Red Cross

22 Revd Dr Mark Durie

23 Centre for Media Transition, UTS

24 Alexander Nilsen

25 Chris Morris

26 *Name withheld*

27 *Submission withdrawn*

28 Linda Jakobson

29 Australian Conservation Foundation

30 The United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, the Special Rapporteur on

the promotion and protection of human rights while countering terrorism, and the Special Rapporteur on the situation of human rights defenders

31 Joint councils for civil liberties

- 31.1 Supplementary

32 The Federation for a Democratic China

33 Professor Rory Medcalf

34 Digital Rights Watch

35 Nyman Gibson Miralis

36 WWF-Australia

37 Chinese Community Council of Australia

38 GetUp

39 350.org Australia

40 Attorney-General

- 40.1 Proposed Government amendments

41 Dr Luke Beck

42 Wal Walker

43 Greenpeace Australia Pacific

44 Joint submission from scholars of China and the Chinese diaspora

45 Eve Trpak and 503 others with similar wording

46 Richard White and 510 others with similar wording

47 Neil Richters and 510 others with similar wording

48 Ric Wallis and 499 others with similar wording

49 Jonathan and Josephine Peter, and 521 others with similar wording

50 Scholars of China, the Chinese diaspora, China-Australian relations and Australia's relations with Asia

51 Whistleblowers Australia

Exhibits

1 *Silent Invasion: China's Influence in Australia*, Clive Hamilton, with research by Alex Joske, January 2018 (unpublished manuscript).

B. List of witnesses appearing at public and private hearings

Monday, 29 January 2018 (private hearing)

Parliament House, Canberra

Attorney-General's Department

- Ms Anna Harmer, First Assistant Secretary, Security and Criminal Law Division
- Ms Tara Inverarity, Assistant Secretary
- Ms Laura Marson, Director

Australian Federal Police

- Assistant Commissioner Debbie Platz
- Commander Justine Gough
- Mr Tony Alderman, Manager, Government and Communications

Australian Security Intelligence Organisation

- Mr Peter Vickery, Deputy Director-General
- Dr Wendy Southern, Deputy Director-General
- First Assistant Director-General, Office of Legal Counsel
- First Assistant Director-General, Counter-Espionage and Interference
- Director

Tuesday, 30 January 2018 (public hearing)

Parliament House, Canberra

Law Council of Australia

- Mr Arthur Moses, President-elect
- Mr Morry Bailes, President
- Dr Natasha Molt, Deputy Director of Policy
- Ms Alice Macdougall

Human Rights Law Centre

- Dr Aruna Sathanapally, Director of Legal Advocacy
- Ms Hannah Ryan, Lawyer

Individuals

- Mr Peter Jennings

Joint media organisations

- Mr Paul Murphy, Chief Executive, Media, Entertainment and Arts Alliance (MEAA)
- Ms Georgia-Kate Schubert, Head of Policy and Government Affairs, News Corp Australia
- Mr Bruce Meagher, Group Director, Corporate Affairs, Foxtel
- Ms Holly Brimble, Manager, Policy and Regulatory, Australian Subscription Television and Radio Association (ASTRA)
- Ms Sarah Waladan, Head of Legal and Regulatory Affairs, Free TV Australia

Wednesday, 31 January 2018 (public hearing)

Parliament House, Canberra

Attorney-General's Department

- Ms Anna Harmer, First Assistant Secretary, Security and Criminal Law Division
- Ms Tara Inverarity, Assistant Secretary
- Ms Laura Marson, Director

Australian Federal Police

- Ms Debbie Platz, Assistant Commissioner, Crime Operations
- Mr Tony Alderman, Manager, Government and Communications

Australian Human Rights Commission

- Mr Edward Santow, Human Rights Commissioner
- Mr John Howell, Lawyer

Australian Security Intelligence Organisation

- Mr Peter Vickery, Deputy Director-General
- Dr Wendy Southern, Deputy Director-General

Department of Home Affairs

- Ms Kelly Williams, Acting First Assistant Secretary, National Security and Law Enforcement Division, Policy Group

Individuals

- Professor Clive Hamilton

Office of the Commonwealth Ombudsman

- Ms Jaala Hinchcliffe, Acting Ombudsman
- Ms Doris Gibb, Acting Deputy Ombudsman

Office of the Inspector-General of Intelligence and Security

- Mr Jake Blight, Deputy Inspector-General
- Ms Christina Raymond, Investigation and Review Officer

Thursday, 15 February 2018 (public hearing)

Parliament House, Canberra

Individuals

- Professor Anne Marie Brady

Friday, 16 February 2018 (public hearing)

Parliament House, Canberra

Joint media organisations

- Mr Paul Murphy, Chief Executive, Media, Entertainment and Arts Alliance (MEAA)
- Ms Georgia-Kate Schubert, Head of Policy and Government Affairs, News Corp Australia
- Mr Bruce Meagher, Group Director, Corporate Affairs, Foxtel
- Ms Sarah Kruger, Head of Legal and Regulatory Affairs, Commercial Radio Australia
- Ms Sarah Waladan, Head of Legal and Regulatory Affairs, Free TV Australia

Office of the Australian Information Commissioner

- Mr Timothy Pilgrim, Information Commissioner
- Ms Angelene Falk, Deputy Commissioner

Friday, 16 February 2018 (private hearing)

Parliament House, Canberra

Attorney-General's Department

- Ms Anna Harmer, First Assistant Secretary
- Ms Tara Inverarity, Assistant Secretary
- Ms Laura Marson, Director

Australian Security Intelligence Organisation

- Dr Wendy Southern, Acting Director-General
- Acting Deputy Director-General
- First Assistant Director-General, Counter-Espionage and Interference

Friday, 16 March 2018 (public hearing)

St Andrews Place, East Melbourne

Individuals

- Mr Tony Kevin

Law Council of Australia

- Mr Morry Bailes, President
- Dr David Neal SC, Member, National Criminal Law Committee
- Dr Natasha Molt, Deputy Director of Policy

Human Rights Law Centre

- Dr Aruna Sathanapally, Director of Legal Advocacy
- Ms Hannah Ryan, Lawyer

Joint media organisations

- Mr Paul Murphy, Chief Executive, Media, Entertainment and Arts Alliance (MEAA)
- Ms Georgia-Kate Schubert, Head of Policy and Government Affairs, News Corp Australia

Attorney-General's Department

- Ms Anna Harmer, First Assistant Secretary
- Ms Tara Inverarity, Assistant Secretary
- Ms Laura Marson, Director

Australian Security Intelligence Organisation

- Mr Duncan Lewis, Director-General
- Mr Peter Vickery, Deputy Director-General

C. Comparison between Schedule 2 and ALRC recommendations

Table 3.1 Comparison of the secrecy offences in Schedule 2 to the Bill with recommendations of the Australian Law Reform Commission's *Secrecy Laws and Open Government in Australia* (2009)

ALRC recommendation	Implemented in the Bill?	Government proposed amendments
Recommendation 4–1 Sections 70 and 79(3) of the *Crimes Act 1914* (Cth) should be repealed and replaced by new offences in the *Criminal Code* (Cth)—the 'general secrecy offence' and the 'subsequent disclosure offences'.	Partially. Sections 70 and 79(3) of the Crimes Act are removed, however, section 70 is replicated in proposed section 122.4 of the *Criminal Code*. The Bill creates a range of general	The amendments provide separate offences for non-Commonwealth officers in proposed section 122.4A. This corresponds more closely with the ALRC recommendation for 'subsequent disclosure offences'.

	secrecy offences in sections 122.1 and 122.2 in the *Criminal Code*, but no separate 'subsequent disclosure offences'.	
Recommendation 5–1 The general secrecy offence should require that the disclosure of Commonwealth information did, or was reasonably likely to, or intended to: (a) damage the security, defence or international relations of the Commonwealth; (b) prejudice the prevention, detection, investigation, prosecution or punishment of criminal offences; (c) endanger the life or physical safety of any person; or (d) prejudice the protection of public safety.	Partially. In addition to disclosures, proposed sections 122.1 and 122.2 also include offences for 'other dealings'; removing from, or holding information outside, a 'proper place of custody'; and failing to comply with a lawful direction. The four essential public interests identified by the ALRC are reflected in proposed sections 122.1 and 122.2. However, section 122.1 creates offences in relation to 'inherently harmful information', which includes security classified information; information relating to intelligence agencies and the operations, capabilities and technologies of law enforcements agencies; and information provided to the Commonwealth by a person under	The concept of 'inherently harmful information' is retained but reduced in scope to exclude security classified information below 'secret' and to exclude information provided to the Commonwealth by a person under a legal obligation. The scope of section 122.2 is reduced to exclude civil penalty provisions, harm or prejudice to Commonwealth-State relations, and harm or prejudice to international relations other than in relation to information that is communicated by a foreign government in confidence. For non-Commonwealth officers, proposed section 122.4A applies to a further limited range of conduct.

	a legal obligation. Section 122.1 does not require any specific harm to occur, or be likely or intended to occur. Also, section 122.2 extends the interests identified by the ALRC to include civil penalty provisions, certain functions of the Australian Federal Police, and Commonwealth-State relations.	
Recommendation 5–2 The terms 'security' and 'international relations' should be defined for the purposes of the general secrecy offence by reference to the relevant provisions of the *Australian Security Intelligence Organisation Act 1979* (Cth) and the *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth).	Partially. Proposed section 121.1 defines 'international relations' by reference to the *National Security Information (Criminal and Civil Proceedings) Act 2004*. The word 'security' is not defined, and the phrase 'security or defence of Australia' is defined without reference to the *Australian Security Intelligence Organisation Act 1979*.	No impact.
Recommendation 6–1 The general secrecy offence should regulate the conduct of those who are, or have been, 'Commonwealth officers', defined as follows:	Partially. The proposed secrecy offences regulate the conduct of Commonwealth officers and all other persons. 'Commonwealth officer' is defined as	The amendments provide separate offences for non-Commonwealth officers in proposed section 122.4A. The existing offences in the Bill are limited to current and former

(a) the Governor-General; (b) ministers and parliamentary secretaries; (c) Australian Public Service employees, that is, individuals appointed or engaged under the *Public Service Act 1999* (Cth); (d) individuals employed by the Commonwealth otherwise than under the Public Service Act; (e) members of the Australian Defence Force; (f) members or special members of the Australian Federal Police; (g) individuals who hold or perform the duties of an office established by or under a law of the Commonwealth; (h) officers or employees of Commonwealth authorities; (i) individuals who exercise powers, or perform functions, conferred on them by or under a law of the Commonwealth;	(a) an APS employee; (b) an individual appointed or employed by the Commonwealth otherwise than under the *Public Service Act 1999*; (c) a member of the Australian Defence Force; (d) a member or special member of the Australian Federal Police; (e) an officer or employee of a Commonwealth authority; (f) an individual who is a contracted service provider for a Commonwealth contract; (g) an individual who is an officer or employee of a contracted service provider for a Commonwealth contract and who provides services for the purposes (whether direct or indirect) of the Commonwealth contract. The Governor-General is excluded from the definition.	Commonwealth officers, consistent with the ALRC recommendation. There is no amendment to the definition of 'Commonwealth officer'.

(j) individuals and entities who are contracted service providers for a Commonwealth contract; or (k) individuals who are officers or employees of a contracted service provider for a Commonwealth contract and who provide services for the purposes (whether direct or indirect) of the Commonwealth contract.		
Recommendation 6–2 The general secrecy offence should regulate the disclosure of Commonwealth information as defined in Recommendation 6–3.	Yes.	No impact.
Recommendation 6–3 The general secrecy offence should apply to any information to which a person has, or had, access by reason of his or her being, or having been, a Commonwealth officer as defined in Recommendation 6–1.	Yes. Proposed sections 122.1 and 122.2 are limited to information was made or obtained by the person, or any other person, by reason of his or her being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity.	The phrase 'or any other person' is removed from proposed sections 122.1 and 122.2. Proposed new section 122.4A is limited to information that was made or obtained by another person by reason of that other person being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity.

Recommendation 6–4 The general secrecy offence should require intention as the fault element attaching to the physical element consisting of disclosure.	Yes. Due to the operation of section 5.6 of the *Criminal Code*, intention is the fault element applying to the conduct in proposed sections 122.1 and 122.2.	No impact.
Recommendation 6–5 The general secrecy offence should require that a Commonwealth officer knew, intended that, or was reckless as to whether, the disclosure of Commonwealth information would harm, or was reasonably likely to harm, one of the public interests set out in Recommendation 5–1.	Partially. Due to the operation of section 5.6 of the *Criminal Code*, recklessness is the fault element applying to the circumstance of information being 'inherently' harmful information' (proposed section 122.1) and the result of the conduct 'causing harm to Australia's interests (proposed section 122.2). As noted above, the Bill expands on the public interests set out by the ALRC in Recommendation 5.1.	No impact.
Recommendation 6–6 There should be a new offence in the *Criminal Code* (Cth) for the subsequent unauthorised disclosure of Commonwealth information where:	No. The Bill does not provide for any separate 'subsequent unauthorised offence' in relation to non-	The amendments provide separate offences for non-Commonwealth officers in proposed section 122.4A. In addition to disclosures (i.e. communications), proposed section

(a) the information has been disclosed by Commonwealth officer A to B (not a Commonwealth officer) in breach of the general secrecy offence; and (b) B knows, or is reckless as to whether, the information has been disclosed in breach of the general secrecy offence; and (c) B knows, intends or is reckless as to whether the subsequent disclosure will harm—or knows or is reckless as to whether the subsequent disclosure is reasonably likely to harm—one of the public interests set out in Recommendation 5–1.	Commonwealth officers.	122.4A also includes an offence for 'other dealings'. Proposed section 122.4A applies in relation to information that • was made or obtained by another person by reason of that other person being, or having been, a Commonwealth officer or otherwise engaged to perform work for a Commonwealth entity; and • has a security classification of secret or top secret; or information for which the communication (or other dealing) damages the security or defence of Australia; interferes with or prejudices the prevention, detection, investigation, prosecution or punishment of a criminal offence; or harms or prejudices the health or safety of the Australian public. Due to the operation of section 5.6 of the *Criminal Code*, recklessness is the fault element applying to these circumstances. The offence does not

		explicitly require the information to have been disclosed to the non-Commonwealth officer in breach of another secrecy offence.
Recommendation 6–7 There should be a new offence in the *Criminal Code* (Cth) for the subsequent unauthorised disclosure of Commonwealth information where: (a) the information has been disclosed by Commonwealth officer A to B (not a Commonwealth officer) on terms requiring it to be held in confidence; (b) B knows, or is reckless as to whether, the information has been disclosed on terms requiring it to be held in confidence; and (c) B knows, intends or is reckless as to whether the subsequent disclosure will harm—or knows or is reckless as to whether the subsequent disclosure is reasonably likely to harm—one of the public interests set out in	No. The Bill does not provide for any separate 'subsequent unauthorised offence' in relation to non-Commonwealth officers.	As above. The offence in proposed section 122.4A does not explicitly require the information to have been disclosed to the non-Commonwealth officer in terms requiring it to be held in confidence.

Recommendation 5–1.		
Recommendation 7–1 The general secrecy offence should expressly include exceptions applying where the disclosure is: (a) in the course of a Commonwealth officer's functions or duties; (b) in accordance with an authorisation given by an agency head or minister that the disclosure would, on balance, be in the public interest; or (c) of information that is already in the public domain as the result of a lawful disclosure.	Partially. There are no exceptions in the physical elements of the secrecy offence. Proposed section 122.5 provides offence-specific defences (for which the defendant bears an evidential burden) in relation to a Commonwealth officer's powers, functions and duties; conduct in accordance with an arrangement or agreement with the Commonwealth (sub section 1); and information that has already been communicated or made available to the public with the authority of the Commonwealth (subsection 2). Proposed section 122.5 also provides defences in relation to communications to the Inspector-General of Intelligence and Security, the Commonwealth Ombudsman and the Law Enforcement Integrity Commission (subsection 3); communications in accordance with the *Public Interest Disclosure Act 2013*	The amendments propose to amend the defence at subsection 122.5(7) to apply where (a) the person dealt with or held the information in their capacity as a person engaged in reporting news, presenting current affairs or expressing editorial content in news media; and (b) at that time, the person reasonably believed that dealing with or holding the information was in the public interest.

	(subsection 4); to a court or tribunal (subsection 5); communications in the public interest in a person's capacity as a journalist engaged in fair and accurate reporting (subsection 6); communication of information that has been previously communicated for which the person believes on reasonable grounds that the further communication will not cause harm to Australia's interests, or the security or defence of Australia (subsection 8); and dealing with information relating to person to or by that person, or with the person's consent (subsection 9).	
Recommendation 7–2 The subsequent disclosure offences should include an exception where the disclosure is of information that is already in the public domain as the result of a lawful disclosure.	N/A. The Bill does not provide for any separate 'subsequent unauthorised offences' in relation to non-Commonwealth officers.	The defences at subsections 122.5(2) and 122.5(8) in relation to previously communication information will apply to the separate 'subsequent disclosure' offences proposed to be inserted at section 122.4A.
Recommendation 7–3 In developing public interest disclosure legislation	N/A. The public interest disclosure	No impact.

the Australian Government should ensure that the legislation protects: (a) individuals subject to the general secrecy offence; (b) individuals who subsequently disclose Commonwealth information received by way of a protected public interest disclosure; and (c) individuals subject to the subsequent disclosure offence for the unauthorised disclosure of information received from a Commonwealth officer on terms requiring it to be held in confidence.	legislation was finalised subsequently to the ALRC report, with the passage of the *Public Interest Disclosure Act 2013*. As noted above, subsection 122.5(4) provides a defence to the secrecy offences for communications in accordance with the *Public Interest Disclosure Act 2013*.	
Recommendation 7–4 The general secrecy offence should stipulate a maximum penalty of seven years imprisonment, a pecuniary penalty not exceeding 420 penalty units, or both.	No. The offences at proposed sections 122.1 and 122.2 stipulate maximum penalties of 15 years for the underlying offences, and 20 years for aggravated offences (see proposed section 122.3).	No impact.
Recommendation 7–5 The subsequent disclosure offences should stipulate maximum penalties of seven years imprisonment, a pecuniary penalty not	No. The offences at proposed sections 122.1 and 122.2—which would apply equally	The amendments provide separate offences for non-Commonwealth officers in proposed section 122.4A. The maximum penalty for these

exceeding 420 penalty units, or both.	to subsequent disclosures—stipulate maximum penalties of 15 years for the underlying offences, and 20 years for aggravated offences (see proposed section 122.3).	offences is 10 years imprisonment, with no applicable aggravating factors.
Recommendation 7–6 The general secrecy offence and the subsequent disclosure offences should provide that, where a court is satisfied that a person has disclosed, or is about to disclose, information in contravention of the provisions, the court may grant an injunction to restrain disclosure of the information.	Yes. Proposed section 123.1 provides that the secrecy provisions will be enforceable under Part 7 of the *Regulatory Powers (Standard Provisions) Act 2014*, which creates a framework for using injunctions to enforce provisions.	No impact.