Submission to the Parliamentary Joint Committee of Intelligence and Security

Review of the Defence Amendment (Safeguarding Australia's Military Secrets) Bill 2023

Outline and Summary

Thank you for the opportunity to make a submission to the public consultation on the proposed Review of the Defence Amendment (Safeguarding Australia's Military Secrets) Bill 2023 ("the SAMS").

This submission has been prepared in my capacity as a Senior Research Fellow of the T.C. Beirne School of Law at the University of Queensland.

However, the views expressed below are entirely my own and are not representative of the School of Law, The University of Queensland or any other government, organisation or agency.

I am happy to provide further clarification on any area of the submission.

The aim of the Bill is to amend the *Defence Act 1903* (Cth) ("Defence Act") to establish a framework to regulate the work that certain former defence staff members (foreign work restricted individuals) can perform without a foreign work authorisation; and the training that Australian citizens and permanent residents, other than foreign restricted individuals, may provide without a foreign work authorisation.

Schedule 1 of the SAMS would insert a new Part IXAA into the Defence Act to regulate work by former Defence personnel. The amended Part IXAA of the Defence Act would commence by defining a "foreign work restricted individual" as any person who was, but is not currently, a defence staff member[1] and is not otherwise covered by an excluding Ministerial instrument.[2]

The SAMS then creates two primary offences and a lesser offence:

- Foreign work restricted individuals who perform work for a foreign military organisation or government body;
- Other individuals (foreign work restricted individuals) who are not providing training to a foreign military organisation or government body, where training relates to goods, software, or technology within the scope of Part 1 of the DSGL; or to military tactics, military techniques, or military procedures; and
- Failing to comply with a condition of a Ministerial work authorisation.

Collectively, these provisions are intended to "bolster Australia's national security by ensuring our military secrets remain safe" and "strengthen the robust laws we have in place by enhancing the Government's ability to prevent the unwanted transfer of sensitive Defence information to foreign militaries".[3]

> *Commendation 1: I **commend** the intention of Parliament to secure Australia's military technology and knowledge from illicit, unintended or unwanted transfers and thefts.*

[1] Amended Act, s 114(1).
[2] Ibid, ss 114(2) and 115(1).
[3] Media Release of the Deputy Prime Minister, the Hon Richard Marles MP, 14 September 2023 <https://www.minister.defence.gov.au/media-releases/2023-09-14/new-legislation-safeguard-australias-military-secrets>.

However, I am also of the opinion that SAMS simply cannot be passed in its present form.

SAMS contains sweeping, vague and incredibly punitive provisions with no logical, rational or observable connection to "military secrets", which is the supposed policy harm which it is intended to remedy. The proposed amendments also unnecessarily expose former ADF members and APS staff to significant potential criminal penalties for merely exercising their rights to seek employment for an entity which resides outside Australia. In doing so, SAMS unfairly elevates the Minister to acting as the arbiter of the circumstances in which, and conditions which will apply to, former ADF member or APS staff seeking employment for government and military agencies outside Australia.

> *Recommendation 1: I **recommend** that SAMS not be passed in its present format and be significantly amended prior to any future re-introduction to Parliament.*

Overlap between section 115A offence with foreign interference and espionage offences

The proposed offence in section 115A of SAMS has significant overlap – thus creating the possibility of duplicity in the criminal law – in respect of other national security offences:

Reckless foreign interference ("RFI"), s 92.3(1)	**Reckless as to national security espionage, s 91.2(2)**
(1) Engages in conduct; (2) On behalf of, in collaboration with, directed, funded or supervised by or on behalf of a foreign principal; (3) Recklessness in relation to the conduct:… prejudice[ing] Australia's national security; (4) Conduct is covert or involves deception.	(1) person deals with information or an article; (2) person is reckless as to whether the person's conduct will prejudice Australia's national security; and (3) the conduct results or will result in the information or article being communicated or made available to a foreign principal or a person acting on behalf of a foreign principal.

Consider a former uniformed member of the ADF or APS member of the Department who, upon their exit from their position, takes up an offer of employment with a foreign corporation providing close protection security services. This employment necessarily draws upon the member's experience in Defence, and the training in tactics, techniques and procedures he or she has received during their service.

Not only is this person engaging in conduct which satisfies all the provisions of the SAMS offence, i.e., by virtue of being a "foreign work restricted individual" and then "working for a foreign military organisation or government body" under the proposed section 115A(1), they also meet three of the proofs for an offence of RFI. Given that it is unlikely that work engaged in by a "foreign work restricted individual" for "foreign military organisation or government body" would be necessarily public information, the proof of "covert" for RFI is necessarily met. The prosecution for an RFI offence only need demonstrate that the work involved recklessness as to a "substantial risk" that the conduct could (but not necessarily would) prejudice Australia's national security.[4]

Similarly, a charge of espionage based on recklessness could also be made out on the same fact scenario. The former ADF member is dealing with "information" obtained during their service, and the

[4] In accordance with standpoint of a reasonable observer at the time of the allegedly reckless conduct, before the outcome was known: *Boughey v R* (1986) 161 CLR 10; *Director of Public Prosecutions v Faure* (1993) 67 A Crim R 172.

conduct results in that information being communicated or made available to a foreign principal. The prosecution need only demonstrate that the dealing with the information was reckless as to the potential prejudice of Australia's national security, in the same sense as the RFI offence.

There is no discernible policy reason for the creation of the section 115A offence, beyond the need to apply the provision to "defence staff members".

It could be suggested that the purpose of the section 115A offence is to remove the proof of an effect (likely or contemplated) that is prejudicial to Australia's national security under existing espionage or national security offences, and instead creating a framework of quasi-strict liability where the defence staff member is exposed to criminal penalties for merely "working" for a foreign military organisation or government body.

If this is the case, Parliament would be better positioned to amend the provisions in the *Criminal Code* rather than creating a new type of offence in the Defence Act.

If Parliament intends to retain section 115A, there should be a more explicit connection between the individual's work for the foreign government which seeks to protect the "military secrets" reposed in the individual.

> *Recommendation 2: I **recommend** that section 115A of SAMS be omitted in its entirety.*
>
> *Recommendation 2A: I **recommend** that if section 115A of SAMS is not omitted, then section 115A(1)(b) of SAMS be amended to include the following:*
>
> *…*
>
> *(b) the individual performs work, where the individual knowledge, skills or experience as a defence staff member, or the kind of information accessed by the individual while a defence staff member, forms a substantial basis, reason or rationale for the work;*
>
> …

Lack of connection with "military secrets"

The most significant challenge to the legitimacy of the SAMS is the lack of any requisite connection between its purported subject matter – the protection of "military secrets", even broadly defined – and the offending conduct which is proscribed. Nowhere in SAMS do the amendments require that an accused deal with information or articles which are properly characterised as "military secrets".

To protect "military secrets", the *Criminal Code* already contains offences relating to information with a security classification.[5] The provision of security classified information to a foreign principal in circumstances of either intention or recklessness as to the effects on Australian national security are considered espionage.[6] A further offence is provided for mere supply of any information with a security classification to a foreign principal.[7] This latter offence does not require the prosecution to prove the accused had in mind a particular foreign principal.[8] Indeed, a prosecution for providing security classified information may be brought against a person irrespective of whether the conduct

[5] Defined as "a classification of secret or top secret that is applied in accordance with the policy framework developed by the Commonwealth for the purpose (or for purposes that include the purpose) of identifying information": *Criminal Code*, s 90.5(1)(a).
[6] *Criminal Code*, ss 91.1(1) and 91.1(2) respectively.
[7] Ibid, s 91.3(1).
[8] Ibid, s 91.3(2).

or its results have any connection with Australia.[9] Mere provision of security classified information to someone not authorised to receive is also an offence.[10]

If a former ADF member or APS staff were to provide security classified information to a foreign principal (irrespective of whether it was undertaken as part of "work" for that foreign principal), they are already liable for prosecution of these offences. If they do so in circumstances where there is recklessness or intentional surrounding the impact on Australian national security, a prosecution for espionage or foreign interference could also already be open depending on the facts.

Taken another way, an ADF member or APS staff may be prosecuted merely for the act of "working" for any "foreign military organisation or government body", irrespective of whether that work involves military secrets.

Paradoxically, if the SAMS is passed in its present form, it will have the somewhat ridiculous effect of criminalising defence staff members' dealings with information that is either unclassified information (because a security classification is a necessary element for a secrecy offence under section 91.3(1) or s 122.1(1) of the *Criminal Code*), or dealings with information that has no effect on Australian national security (as a prejudicial effect on national security is a necessary element for an espionage or foreign interference offence under the *Criminal Code*).

For those reasons, the section 115A and 115B offences proposed in SAMS ought to be amended to apply only to any situation where a former ADF member or Departmental APS discloses, uses, disseminates or communicates "military secrets".

> *Recommendation 3: I **recommend** that sections 115A and 115B of SAMS be amended to include a new subsection (1A) under "Exceptions" that states:*
>
> *(1A) Subsection (1) does not apply if the work performed by the individual does not involve, rely upon, utilise, communicate, or disseminate information that has a security classification.*
>
> *Note: See the definition of **security classification** in section 90.5 of the Criminal Code.*

Duplication of existing official secrets prohibitions

Section 115A of SAMS further highlights an ongoing issue the Commonwealth legislature seems to have with so-called "official secrets" in Australian criminal law.

Prior to 2018, any "Commonwealth officer" – including ADF members and Defence APS – would be exposed to criminal liability if they unlawfully disclosed official information; that is, information obtained or collected by them in the course of their official duties.[11] Such disclosures could be punished by up to 2 years imprisonment; however, if the disclosure was with the "intention of prejudicing the security or defence of the Commonwealth or a part of the Queen's dominions", the maximum penalty increased to 7 years imprisonment.[12]

When the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth) took effect in July 2018, it replaced these "official secrets" provisions with the information dealings provisions in the *Criminal Code*. These provisions were explicitly designed to reflect both international legal opinion, but also the need to ensure that the "gravity of the threat posed by the

[9] Ibid, ss 91.7 and 15.4.
[10] Ibid, s 122.1-122.4A.
[11] *Crimes Act 1914* (Cth), s70, as in force prior to July 2018.
[12] Ibid, s 79.

disclosure of inherently harmful information or information which causes or will cause harm to Australia's interests" was properly proscribed.[13]

The Explanatory Memorandum made clear that the new provisions – contained in the new Division 122 of the *Criminal Code* – would provide clarity and certainty to Commonwealth officials and their information-handling duties:[14]

> *The drafting of section 70 is outdated and complicated, resulting in a lack of clarity about the scope of the offence… Part VII of the Crimes Act (Official secrets and unlawful soundings) contains a range of offences relating to official secrets, prohibited places and unlawful soundings…*
>
> *There have been calls for significant reforms to Parts VI and VII for many years. In particular, the Australian Law Reform Commission's 2010 Report, Secrecy Laws and Open Government in Australia (Report 112) concluded that there are 'real concerns' with the operation of the existing offences, which are 'out of step with public policy developments in Australian and internationally'. Additionally, the drafting of the current offences is outmoded. As a result, it can be challenging for persons to understand when they will be subject to criminal liability, and for bring successful prosecutions.*

The new sections 122.1 to 122.4 of the *Criminal Code* created offences relating to various dealings with "harmful information", with a variety of constructions relating to Australia's national security, international relations, Defence, law enforcement, or the health and safety of members of the public.[15] At their most serious, a conviction for this offence is punishable by up to 7 years (increasing to 10 years if circumstances of aggravation are present[16]). ADF personnel and Defence APS attracted a higher penalty for these offences because they "have a higher duty to protect such information, should be well trained in security requirements procedures and, in many cases, have security clearances".[17]

The gap – such that one exists – is actually only in the definition of "inherently harmful information" in the *Criminal Code* as applying to unlawful disclosure of information offences.

If that definition were amended to include (as an example) "information relating to the operations, capabilities or technologies of, or methods or sources used by the Australian Defence Force or Department of Defence", then a disclosure of such information would *prima facie* amount to an offence. If the person held a security clearance at the time, they are also exposed to the aggravated form of the offence.

Such a construction has a far more appealing connection to the protection of "military secrets" than the creation of an entirely new offence in the Defence Act as proposed.

> *Recommendation 4: I **recommend** that instead of passing section 115A of SAMS, the definition of "inherently harmful information" in section 121.1 of the Criminal Code should be amended to include the following:*

---

[13] Explanatory Memorandum to the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2018, 28 at [121]-[122].
[14] Ibid, 255 at [1224]-[1226].
[15] *Criminal Code*, s 121.1.
[16] Ibid, s 122.3.
[17] Explanatory Memorandum to the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2018, 29 at [124].

*"**inherently harmful information**" means information that is any of the following:*

…

(f) information relating to the operations, capabilities or technologies of, or methods or sources used by the Australian Defence Force or Department of Defence;

…

Overlap of section 115B offence with export control laws

Section 115B offence of SAMS will apply to any person – not being a formerly defence staff member – who supplies training to a foreign principal which is based on either goods, software, or technology within the scope of Part 1 of the Defence and Strategic Goods List; or the training relates to military tactics, military techniques or military procedures.

Supply or brokerage of DSGL technology (including Part 1) is already an offence under the *Defence Trade Controls Act 2012* (Cth),[18] as is the publication of any technology in Part 1 of the DSGL,[19] if the person does not hold a permit to do so.

If passed in its present form, SAMS will have the effect of punishing the supply of training regarding DSGL technology with imprisonment of up to 20 years imprisonment, but not the supply of the technology itself, which is punishable by only 10 years imprisonment.

A reasonable question could be asked whether SAMS will incentivise potential offenders to preference the supply or brokerage of DSGL technology to foreign governments or entities, as that conduct attracts a lesser penalty.

Another question could also be asked whether the policy harm – and therefore the size of the deterrence to be attached to that harm – comes from supplying training on DSGL technology, or the supply and brokerage of that technology instead.

*Recommendation 5: I **recommend** that section 115B of SAMS be omitted in its entirety.*

*Recommendation 5A: I **recommend** that if section 115B of SAMS is not omitted, then the proposed maximum penalty of an offence under section 115B(1) of SAMS is punishable by a maximum penalty of up to 10 years imprisonment to better align it with other like offences.*

Unintended consequences of prohibiting training "relating to military tactics, military techniques or military procedures"

Section 115B of the proposed SAMS would also proscribe training "relating to military tactics, military techniques or military procedures", where the training is supplied to a "relevant foreign country". Exemptions are provided for persons covered by a foreign work authorisation, persons authorised by a written agreement to which the Commonwealth is a party, or training supplied as part of official duties of the Commonwealth. However, military tactics, military techniques or military procedures is not defined in the SAMS, nor the broader Defence Act.

There are two significant problems with the proposed wording.

The first problem is that by not defining "military tactics, military techniques or military procedures" it is impossible for the average person to understand whether they might be committing an offence.

[18] *Defence Trade Controls Act 2012* (Cth), ss 10(1) and 15(1).
[19] Ibid, s 14A(1).

A crucial aspect of the rule of law is that the law is known and predictable so that all people can be guided by it and know clearly the consequence of their actions.

Consider the following hypothetical scenarios:

- A history professor delivers a lecture to a Vietnamese university about Australian military tactics used during the Vietnam War;
- An entrepreneur delivers a presentation to a Chinese trade delegation that references their organisation's "military-inspired" leadership structure;
- A person teaching a journalism course at a Swedish government facility describes the platoon activities of a unit of Australian Special Air Service (SAS) operators revealed as part of a war crimes investigation.

Are these persons the offenders which this legislation intends to capture? Put a different way, are these disclosures related to the "military secrets" which the SAMS intends to protect? There must be a relevant "military secret" in need of protecting to which the offence under section 115B(1) must be directed.

Although I anticipate that – should SAMS become law – the Minister will make a legislative instrument under section 115(3) which contains an exhaustive list of countries which are exempted from being "relevant foreign countries" for the purpose of SAMS, and thus exclude most of the above hypotheticals. However, this does not address the fundamental problem with SAMS effectively proscribing <u>any</u> work for a foreign country where that work has no requisite connection to "military secrets".

The second problem with this provision in SAMS is that the ordinary meaning of "military tactics, military techniques or military procedures" can carry unique connotations in the digital battlegrounds of contemporary conflict. For example, given that off-the-shelf drones are being used as weapons of warfare in the Russia-Ukraine conflict,[20] does a person commit an offence by training drone piloting to foreign entities? Do cybersecurity techniques – such as vulnerability assessment or network penetration testing – count as "military techniques" if they are used by the military in conflicts?[21]

SAMS should be amended to include an explicit definition of "military tactics, military techniques or military procedures", such that the ambiguity relating to such questions does not expose innocent persons to potential criminal offences with such significant penalties of imprisonment.

> *Recommendation 6: I **recommend** that an exception be included such that section 115B(1) does not apply if it relates to training in "military tactics, military techniques or military procedures that have already been communicated or made available to the public".*
>
> *Recommendation 7: I **recommend** that an explicit definition of "military tactics, military techniques or military procedures" be included in section 113 of SAMS.*

Lack of safeguards for commencement of prosecution

As outlined in the previous section, there is a significant overlap between the proposed offences under the amended sections 115A and 115B of the Defence Act, and other Commonwealth national security offences. Indeed, the Explanatory Memorandum makes clear that this is in fact an intended

[20] Andrew Kramer, "Homemade, Cheap and Lethal, Attack Drones Are Vital to Ukraine", *New York Times* (8 May 2023) <https://www.nytimes.com/2023/05/08/world/europe/ukraine-russia-attack-drones.html>.
[21] *Defence Cyber Security Strategy* (Report, 31 August 2022) <https://www.defence.gov.au/about/strategic-planning/defence-cyber-security-strategy>.

consequence of the legislation.[22] The Explanatory Memorandum also makes clear that Parliament's intention is to frame the offences as carrying "an effective deterrent and reflects the seriousness of the offence".[23]

However, it is also clear from the SAMS that the Commonwealth (or its agents) may prosecute alleged offences under sections 115A, 115B and 115D without requiring the express written consent of the Attorney-General.

Requiring the Attorney-General's consent for the prosecution of national security offences is an important safeguard built into the *Criminal Code* for other crimes such as training foreign military forces,[24] as well as sabotage,[25] espionage,[26] bribing a foreign official,[27] and unlawful disclosure of information.[28] The oversight of the Attorney-General means that only those prosecutions that are both in the public interest and capable of meeting the stringent and complex legal requirements of the *Criminal Code* are continued at taxpayer expense.

Although the consent of the Attorney-General is required for the prosecution of any offences which exercise extended geographical jurisdiction[29] (which apply Category B jurisdiction to the offences under sections 115A, 115B and 115D of the amended Act[30]), the Attorney-General's consent is not required to prosecute a person who works for, or provides military training to, a foreign military organisation or government body where the accused's conduct or result of the conduct occurs within Australia.

The Attorney-General's express written consent should be a requirement prior to the prosecution of any SAMS offences.

> *Recommendation 8: I **recommend** that SAMS be amended to include in Division 5—Other matters the following section:*
>
> xxx.x Requirements before proceedings can be initiated
>
> (1) Proceedings for the commitment of a person for trial for an offence against this Part must not be instituted without:
>
> (a) the written consent of the Attorney-General; and
>
> (b) for proceedings that relate to security classified information--a certification by the Attorney-General that, at the time of the conduct that is alleged to constitute the offence, it was appropriate that the information had a security classification.
>
> (2) However, the following steps may be taken (but no further steps in proceedings may be taken) without consent or certification having been obtained:

---

[22] Explanatory Memorandum to the Defence Amendment (Safeguarding Australia's Military Secrets) Bill 2023, 9 at [63] and 14 at [101].
[23] Ibid.
[24] *Criminal Code,* s 83.5(1).
[25] Ibid, s 82.13(1).
[26] Ibid, s 93.1(1).
[27] Ibid, s 70.5(2).
[28] Ibid, s 123.5(1).
[29] Ibid, s 16.1(1).
[30] Amended Act, ss 115A(7), 115B(7) and 115D(2).

(a) a person may be arrested for the offence and a warrant for such an arrest may be issued and executed;

(b) a person may be charged with the offence;

(c) a person so charged may be remanded in custody or on bail.

(3) Nothing in subsection (2) prevents the discharge of the accused if proceedings are not continued within a reasonable time.

Creation of a serious offence with mixed standards of criminal responsibility

The above hypothetical fact scenario exposes another significant problem with the proposed amendments to the Defence Act – that of intent. The SAMS does not proscribe the fault elements for the various physical elements of the offences under sections 115A, 115B or 115D. This means that the *Criminal Code* imposes a fault element of intention for conduct, and a fault element of recklessness for circumstances or results.[31]

One such result of this lack of clarity is that a person may be reckless as to whether their work is performed for, or on behalf of (a) a military organisation of a foreign country, or (b) a government body of a foreign country. For an offence of such seriousness – and for which the penalty is a potential carceral sentence of up to 20 years – the Act ought to proscribe that all fault elements of the offence are "intentional".

*Recommendation 9: I **recommend** that SAMS be amended to make clear that the fault elements for the offence require proof of intention, i.e., recklessness is not sufficient proof of the elements of the offence.*

Application to <u>all</u> ex-Defence personnel

Another significant concern in the Act regards its application to all ex-serving uniformed personnel (including Reservists) and APS staff of the Department of Defence, irrespective of the time that has elapsed since they worked in a military environment.

The proposed amendments to the Defence Act permit the Minister to exclude from the definition of a "foreign work restricted individual" any person as defined by Ministerial instrument.[32] This provision does explicitly state that the Minister may consider:

(a) particular kinds of work performed by defence staff members;

(b) the period of time that has elapsed since the performance of particular kinds of work by defence staff members.[33]

The clear intention here is to allow the Minister the flexibility to determine that particular types or classes of work performed by defence staff members do not involve or concern the "military secrets" to which this amendment is intended to capture. The further intention is that after a certain period, the information held by defence staff members that was obtained in the course of their official duties will become outdated, superseded, or replaced by more recent information (lowering its utility to a potential adversary).

---

[31] *Criminal Code*, ss 5.6(1) and (2).
[32] Amended Act, ss 114(2) and 115(1).
[33] Ibid, s 115(2).

However, the amendments to the Act do not mandate that these provisions be considered. The Minister has absolute and unappealable discretion to determine what – if any – of the criteria in section 115(2) of the amended Act will apply in the legislative instrument.

> *Recommendation 10: I **recommend** that the Bill be amended such that section 115(2) of the Defence Act require that the Minister "must" (not "may") consider the criteria in sections 115(2)(a) and (b) when making a Ministerial instrument under that section.*

Lack of application to military contractors

A curious outcome of the SAMS relates to the work of Defence subcontractors, whether or not those entities are subcontracted by the ADF or the Department of Defence.

A "foreign work restricted individual" is "an individual who was, but is not currently, a defence staff member", and a "defence staff member" includes senior officers and members of the ADF, Secretary and APS members of the Department of Defence, and the Head and APS members of the Australian Submarine Agency. However, an entity engaged under a contract of services is not included in the definition of "defence staff member".

This seems a curious omission, given the size of the Defence contractor workforce is sizeable,[34] and these contractors may possess identical security clearances and access to "military secrets" as members of the ADF or the Department.

Should the Committee believe that SAMS should be passed, it should be amended to provide clarity that "foreign work restricted individual" includes persons who are engaged by either the ADF or Department under a contract for services.

> *Recommendation 11: I **recommend** that the definition of "defence staff member" in section 113 of SAMS be amended to include:*
>
> ***defence staff member** means:*
>
> *…*
>
> *(d) an employee of any entity that has performed work under a contract for services with the Defence Force, the Department, or the Australian Submarine Agency, and where the employee has performed work for the Defence Force, the Department, or the Australian Submarine Agency because of or subject to that contract for services.*

Size of applicable penalties

Under the amendments to the Act, both offences will carry potential penalties of up to 20 years imprisonment.[35] The lesser offence of failing to comply with a condition of a foreign work authorisation punishable by a penalty of up to 5 years imprisonment.[36]

The size of the penalty for the two primary offences – "foreign work restricted individuals working for a foreign military organisation or government body" and "other individuals providing training to a foreign military organisation or government body" – are significant. In fact, the Explanatory

---

[34] Andrew Tillett, "Defence's army of contractors swallowing up more taxpayers' funds", *Australian Financial Review* (26 May 2021) <https://www.afr.com/politics/federal/defence-s-army-of-contractors-swallowing-up-more-taxpayers-funds-20210525-p57ux1>.
[35] Amended Act, ss 115A(1) and 115B(1).
[36] Ibid, s 115D(1).

Memorandum stipulates that the penalty is intended to "complement comparable offences in other Commonwealth legislation", including by aligning with "penalties imposed by secrecy, sabotage and foreign interference offences under the Criminal Code".[37]

Unfortunately, the statement in the Explanatory Memorandum is somewhat inaccurate. By way of comparison with other offences under Australian national security laws, the possible penalties are:

- Urging violence against the Constitution – 7 years imprisonment;[38]
- Advocating a terrorist act – 5 years imprisonment;[39]
- A Commonwealth official unlawfully communicating information that is inherently harmful information – 7 years imprisonment;[40]
- Reckless sabotage – 15 years imprisonment;[41]
- Reckless foreign interference – 15 years imprisonment.[42]

The penalty is the same as intentional foreign interference,[43] intentionally causing harm to Australian citizens,[44] reckless espionage,[45] or providing military-style training to a foreign principal.[46]

> *Recommendation 12: If recklessness is included as a fault element for section 115A and 115B offences, I **recommend** that the penalties be reduced to 15 years' imprisonment to align with other national security provisions in Australian criminal law.*

Conclusion

I hold some significant concerns with the proposed amendments to the Defence Act, and do not believe that this Bill should be passed in its present form. Although the intention of government to secure our military information is not only to be welcomed but strongly endorsed, there are numerous proposed amendments which do not meet the requisite policy intention of doing so.

Should the Committee consider recommending that SAMS be passed, I urge the Committee to seriously consider the recommendations I have made above.

Thank you for the opportunity to make this submission.

Dr Brendan Walker-Munro, Senior Research Fellow, The University of Queensland

[redacted]

[37] Explanatory Memorandum to the Defence Amendment (Safeguarding Australia's Military Secrets) Bill 2023, 9 at [64]-[65].
[38] *Criminal Code*, s 80.2(1).
[39] Ibid, s 80.2C(1).
[40] Ibid, s 122.1(1).
[41] Ibid, s 82.6(1).
[42] Ibid, s 92.3(1).
[43] Ibid, s 92.2(1).
[44] Ibid, s 115.3(1).
[45] Ibid, s 91.8(2).
[46] Ibid, s 83.3(1).