Australian Government

NATIONAL INTELLIGENCE COMMUNITY

# Submission to the INSLM Review into the operation and effectiveness of the NSI Act

9 JUNE 2023

NIC National Intelligence Community

# Contents

# Executive Summary

The National Intelligence Community (NIC) welcomes the opportunity to make a submission to the INSLM's review into the operation and effectiveness of the *National Security Information (Criminal and Civil Proceedings*) Act 2004 (NSI Act).

In this submission, the NIC makes a strong statement in support of the NSI Act by explaining why and how it achieves an appropriate balance between a range of public interest factors including the need to protect Australia's most sensitive intelligence and security capabilities, operations and people, while ensuring the proper administration of justice.

The context through which the NIC has considered the operation and effectiveness of the NSI Act is the national security threat environment. The Director-General of Security stated in February 2023 that the threats facing Australia are more serious and sophisticated than ever before. Australia is facing an unprecedented challenge from espionage and foreign inference. If left unchecked, this could do serious damage to our sovereignty, values and national interest. And while our National Terrorism Threat Level is POSSIBLE, Australia remains a potential terrorist target; the counter-terrorism mission continues to be challenging and the operational tempo is not diminishing.

While the security environment is complex, challenging and changing, the NIC remains committed to protecting and enhancing Australia's security, prosperity and sovereignty. We will use our collective capability to identify, target and disrupt threats to Australia.

Law enforcement action is a critical weapon in Australia's arsenal to counter and disrupt those who seek to harm us, including through the arrest, charging and prosecution of individuals for terrorism, espionage or foreign interference offences. In this arena, law enforcement outcomes may require collaboration with NIC agencies and the evidence relied upon in proceedings may contain highly sensitive national security information. Operational success, culminating in successful prosecution, relies on being able to do things our adversaries believe are impossible, including the use of highly sophisticated tools, techniques and technologies. The NIC's success also relies on the people working to protect our nation's security, prosperity and sovereignty, some of whom are undeclared so they can do their jobs effectively and safely.

Additionally, a range of administrative decisions may rely on national security information, such as decisions to protect Australia's critical infrastructure and telecommunications systems. The administration of justice is served if those decisions can be reviewed by courts with the best possible evidence.

The other vital asset for Australia and the NIC in seeking to identify, target and disrupt threats to Australia's national security is our relationships with our closest partners and allies. These relationships provide access to unique intelligence, tools, techniques and technologies. This access relies on

relationships of trust and confidence that this intelligence and these tools, techniques and technologies will be protected and will not be exposed without their agreement.

For these reasons, there are circumstances where particularly sensitive information should not be publicly disclosed in a court. The NIC respects and supports the principle of open justice; noting this must be weighed against the need to always protect our people, capabilities and operations to ensure that Australia's national security interests are not compromised.

This submission highlights how the NSI Act has been critical for courts, law enforcement agencies and prosecutors to protect the disclosure of information relating to the NIC's highly sensitive information, capabilities and people in court proceedings.

**Classified and unclassified submission**

The NIC has also provided a classified version of this submission to the INSLM. It is identical to this submission save for the addition of classified case studies, a short amount of classified material regarding current threats; document classification markings and a change to this sentence.

## Summary of key points

a. The NSI Act should be retained because it provides a transparent, consistent and reliable framework for courts to effectively manage the disclosure of national security information in legal proceedings. There may be times, in both civil and criminal cases, where a party needs to rely on sensitive national security information and it is in the public interest to have a mechanism such as the NSI Act for evidence to be safely tendered to enable those cases to proceed. Other legal mechanisms are available to achieve some of the same outcomes but, unlike the NSI Act, do not provide such a comprehensive and effective framework.

b. The framework for balancing public interest factors under the NSI Act is appropriate. Importantly, it ensures that decisions to protect national security information do not seriously interfere with the administration of justice (s. 3(2)) or impinge upon a defendant's right to a fair trial in criminal proceedings. The right to a fair trial is given primacy by s. 19(2) which enables a court to stay a prosecution if protection of national security information would have a substantial adverse effect on that right.

c. The definition of 'national security information' is not too broad and must be broad for the NSI Act to work effectively and to meet a complex and changing environment. National Security, includes security, defence, international relations and law enforcement as these are all intrinsic to the protection of Australia and the Australian people from harm. However, the definition should be amended to more explicitly include two categories commonly featured in NSI cases: operationally sensitive information, and identities of ASIO employees or affiliates and ASIS staff members or

agents. This would promote efficiency, certainty and clarity – and be in line with existing legislative protections.

d. There is no need for the NSI Act to expressly provide for the appointment of a special advocate. These appointments are already possible. They should be 'a last resort' restricted to cases in which a court considers it appropriate to admit national security information as evidence in the proceedings, but not make it available to the other party or their legal representatives. Special advocates should not be appointed to review information that is subject to a claim for public interest immunity because neither the parties nor the court can rely on that material and no unfairness arises for the special advocate to address.

e. It is not necessary for the NSI Act to be more widely available and there may be constitutional impediments to expanding the remit of the NSI Act beyond federal criminal and civil proceedings. The more limited role national security information is likely to play in these jurisdictions means the benefit may be outweighed by the impediments. The NSI Act should not be extended to administrative tribunals, as effective mechanisms for protecting national security information appropriate to the executive nature of these bodies already exist.

f. Maximum sentences under the NSI Act should be brought into line with equivalent offences under the *Australian Security Intelligence Organisation Act 1979* (ASIO Act), the *Intelligence Services Act 2001* (ISA), the *Office of National Intelligence Act 2018* (ONI Act) and the *Criminal Code Act 1995* (Criminal Code) because the conduct and consequences of unauthorised disclosure are at least as serious. This would more effectively deter or punish worst-case offending:

   - The maximum penalty for breaching s. 40 – 45, s. 46, s. 46A – s. 46F and s. 46G of the NSI Act should be increased from 2 to 10 years' imprisonment consistent with s. 39 – s. 40B and s. 41 of the ISA, s. 42 of the ONI Act, s. 18 and s. 92 of the ASIO Act and the aggravated offences under s. 122.1(1) and s. 122.2(1) of the Criminal Code.

   - The maximum penalties for breaching s. 45A and s. 46FA of the NSI Act should be increased from 6 months to 3 – 5 years' imprisonment consistent with s. 40C – 40M of the ISA, s. 44 of the ONI Act, s. 18A – s. 18B of the ASIO Act and the aggravated offences under s. 122.1(2)(3)(4) and s. 122.2(2)(3)(4) of the Criminal Code.

g. The NSI Regulation should be reviewed to include orders now routinely made under s. 22 and s. 38B of the NSI Act. This would modernise the NSI Regulation as a standard for protecting national security information in proceedings. It would also reduce the burden on courts having to rule on routine uncontroversial protections in each case and would ensure transparency through the Regulation being readily available to the public. This may require an amendment to s. 23 and s. 38C of the NSI Act to allow a broader range of matters to be included in the Regulation.

h. The NSI Act should be amended to enable the protection of NSI in anticipation of legal proceedings. This will enable intelligence agencies to disclose information earlier and promote settlement of suitable matters prior to the commencement of proceedings.

i. The NSI Act should be amended to restrict appeals under Part 3 Division 4 and Part 3A Division 4 of the NSI Act to questions of law. Limiting appeals to questions of law will ensure consistency and minimise delay.

j. Consideration should be given to the feasibility of establishing a National Security Division of the Federal Court, or equivalent in relevant State and Territory jurisdictions, to hear cases in which the NSI Act has been invoked. This would be particularly valuable if it enabled the development of a secure facility (or facilities) and associated infrastructure and expertise among court staff for creating, storing, handling and communicating national security information and conducting hearings in an appropriately secure environment.

# Introduction

2. This submission reflects the shared views of the entire National Intelligence Community (NIC) including:

- the Office of National Intelligence (ONI);
- the Australian Security Intelligence Organisation (ASIO);
- the Australian Secret Intelligence Service (ASIS);
- the Defence Intelligence Organisation (DIO);
- the Australian Geospatial Intelligence Organisation (AGO);
- the Australian Signals Directorate (ASD);
- the Australian Federal Police (AFP);
- the Department of Home Affairs;
- the Australian Criminal Intelligence Commission (ACIC); and
- the Australian Transaction Reports and Analysis Centre (AUSTRAC).

3. The submission is based on nearly twenty years of shared experience in agencies that have engaged with the NSI Act on a broad range of legal matters in various jurisdictions, including in both civil and criminal proceedings. It also draws on our experience managing the disclosure of national security information in legal proceedings where the NSI Act was either not invoked or was not available.

4. In preparing this submission the NIC consulted with the Department of Foreign Affairs and Trade, the Attorney General's Department and the Commonwealth Director of Public Prosecutions. As the AFP has equities as both a law enforcement agency involved in the criminal investigation and prosecution process, and an agency with an intelligence function, the AFP will also make a separate submission to the Review.

# Balancing Public Interests

5. The NIC understands and supports the importance of open justice; however, this needs to be balanced against risks of compromising national security. There are circumstances where particularly sensitive information cannot be disclosed in open court, or even sometimes in a closed court, for public interest reasons.

6. As members of the NIC, we are entrusted to protect our nation and its people from those who would do us harm – including by identifying and prosecuting spies, saboteurs and terrorists; those engaged in covert acts of foreign interference; or other criminal conduct designed to harm Australia's national interests. We are acutely aware of how fragile our security can be and the need to protect our operations, methods, sources and intelligence; as well as that shared with us by our partners and allies. We know how the disclosure of (sometimes even seemingly innocuous) information can compromise our capabilities, undermine our relationships with key partners, damage Australia's global standing, compromise intelligence operations and put lives at risk. We have seen first-hand the consequences of the unlawful disclosure of classified information. A single release can undermine many years of focused effort.

7. We must protect our people, capabilities and operations. People are our most important capability and some members of the NIC (e.g. ASIS and ASIO officers) remain undeclared for their safety. It is also vital to safeguard the tools, techniques and technologies that allow us to do things that Australia's adversaries do not expect. We must also protect our operations, or we tip off our targets and potentially reveal our people and our capabilities.

8. We understand the importance of Australia's international relationships to the protection of Australia and its people and the future prosperity of our country and region. Australia's cooperation with its partners and allies is integral to this. Our operating environment is an international one and we need to maintain the confidence of Australia's partners and allies.

9. We are also mindful of the public interest in the administration of justice. This includes ensuring that relevant and admissible evidence bearing on the guilt or innocence of an accused is available to the court (see *Sankey v Whitlam* (1978) 142 CLR at 42) and protecting the integrity of our justice system by proceedings remaining as open and transparent as possible. We agree that legal proceedings (including proceedings involving matters of national security) should be conducted in public, except where it is necessary to do otherwise to secure the proper administration of justice (see French CJ in *Hogan v Hinch* [2011] HCA 4 at [21]-[22]).

10. The balancing exercise undertaken by the court of the public interests should not be characterised as a binary contest between the Government (intent on closing proceedings to protect national secrets) and individuals (interested in open justice and a fair trial). The court's role is to balance *a range of factors* to determine what is in the *public interest*. The Australian Law Reform Commission summed up well the difficulty in its May 2004 'Keeping Secrets' Report when it said:

> The ALRC's challenge in this inquiry was to develop a mechanism capable of reconciling, so far as possible, the tension between disclosure in the interests of fair and effective legal proceedings, and non-disclosure in the interests of national security. It would be an oversimplification, however, to characterise the task as striking a balance between the right of an *individual* to fair and open trial with the need of the *Government* to maintain official secrets. Due consideration and weight must be given to the broader and compelling *public* interests in safeguarding national security and strategic interests; facilitating the successful prosecution of individuals who engage in acts of terrorism or espionage; maintaining the fundamental fairness, integrity and independence of our judicial processes; and adhering, to the greatest extent possible, to the principles and practices of open justice and open and transparent government.

# The Current Threat Environment

11. In his 2023 Annual Threat Assessment, the Director-General of Security described the current security environment as complex, challenging and changing:

> 'Complex' because the threats are increasingly intersecting, emerging from new places and blurring traditional distinctions. A foreign power can simultaneously be interfering, spying, and setting up for sabotage.
>
> 'Challenging', because Australia is being targeted by sophisticated foreign adversaries that are effectively unconstrained by resources, ethics and laws, and they carefully hide their activities.
>
> 'Changing', because threats are shaped by shifting geopolitics, emerging technologies, and broader social trends that include online radicalisation and the growth in extreme views, conspiracies and grievances.

12. Australia is facing an unprecedented challenge from espionage and foreign interference, and the threats are more serious and sophisticated than ever before. Foreign intelligence services are seeking to penetrate government, defence, academia and business to steal classified information, military capabilities, policy plans and sensitive research and innovation. They are targeting all levels of government, intimidating members of diaspora communities and seeking to interfere in our democratic institutions.

13. In the last year, a small number of Australian legal figures have been subjected to suspicious approaches. While we are yet to conclusively conclude they were targeted by foreign intelligence

services, we do know spies want insights into court cases relevant to their governments and are seeking to use litigation as an intelligence collection tool. Foreign spies have been brazen in the United States recently, seeking to obstruct prosecutions and manipulate outcomes.

14. Australia's open and transparent court process could enable our foreign adversaries to use the court process to try and 'look behind the curtain' of classified capabilities and information.

15. In 2004, when the ALRC handed down its report and the NSI Act was introduced into parliament, Australians were living in a very different threat environment than they are now. The ALRC stated at the time that 'cases involving espionage, terrorism and the leaking and misuse of national security information have been – and hopefully will remain - quite rare in Australia'. That is no longer the case, with national security case numbers expected to increase in a deteriorating threat environment.

16. In the current threat environment, it has never been more important to have an appropriate framework through which:

a. courts can effectively manage the disclosure of national security information in legal proceedings to ensure that it is protected where it needs to be and stored and handled appropriately by those entrusted with it; and

b. the Commonwealth can confidently prosecute those engaged in terrorism, espionage or foreign interference, or other conduct contrary to the national interest and bring or respond to civil claims without fear that the legal process will be used to undermine Australia's national security.

17. It is essential to have an Act, like the NSI Act, to achieve these objectives. Repealing or winding back the NSI Act will make it more difficult (if not, in some cases, impossible) to achieve them and will send the wrong message to hostile foreign intelligence services: that the Australian legal system is becoming a more attractive environment for targeting judges, lawyers, counsel, court staff, transcribers and others with access to national security information. It will also send the wrong message to our partners and allies: that they should think twice before sharing their most sensitive intelligence and capabilities with us because they will be at greater risk of disclosure in legal proceedings.

# Responses to matters identified by the INSLM

1. Whether the interaction of the protection of national security information and the public adjudication of disputes according to law would better occur if the *NSI Act* were repealed. In particular, whether powers available to courts, in the absence of the *NSI Act*, can more appropriately deal with this interaction than the processes required by the *NSI Act*.

18. The interaction of the protection of national security information and the public adjudication of disputes according to law would not better occur if the NSI Act were repealed.

## Why the NSI Act Was Necessary

19. The NSI Act was passed following the stayed prosecution of Simon Lappas, a Defence Intelligence Officer who allegedly provided classified documents sourced from a foreign power to an associate, Sherryl Dowling, with the intent that they be sold to a second foreign power. The prosecutor in that case sought to: rely on 'shells' of the classified documents, indicating their format and 'Top Secret' classification; and to adduce evidence in general terms only of their contents and usefulness to a foreign power. The prosecutor was unable to tender the original documents because the foreign power that owned the classified information would not agree to it to being shown to the jury. It became apparent midtrial that this course was not open to the prosecutor and the only way to protect the classified information was to claim public interest immunity. Once public interest immunity was claimed, the documents could not be used as evidence and one of the charges against Mr Lappas was permanently stayed: *R v Lappas and Dowling* [2001] ACTSC 115. This 'all or nothing' approach to protecting national security prevented the trial of a serious charge and was not in the interests of justice.

20. In the absence of an act, such as the NSI Act, to promote the early identification and resolution of issues relating to the disclosure of national security information, it was more likely that they would arise unexpectedly during a trial, often after inappropriate disclosures had been made, meaning that claims for public interest immunity were determined at very short notice, to the inconvenience of both the Court and the parties. Additionally, public interest immunity did not protect national security information from disclosure prior to the making of a court order. Nor did it allow for summaries or stipulations of fact to be substituted. Section 130 of the *Evidence Act 1995*, which conferred a statutory equivalent of the common law right to make public interest immunity claims, operated in much the same way and suffered from some of the same deficiencies. In addition, s. 130 did not apply to all jurisdictions and its application was limited to the trial stage of a proceeding.

21. Following the *Lappas* case, the issue was referred to the ALRC which stated:

> At present, the admissibility or otherwise of classified and security sensitive information is usually tested through a claim for public interest immunity. After hearing all of the arguments in a particular case, the court might rule that the classified and security sensitive information must be admitted into evidence in open court (despite the risk of adverse consequences for Australia's national security), or that the classified and security sensitive information must be completely excluded (despite the difficulties this may present to the defendant or non-government party).

22. This effectively put the Commonwealth in the position of having to 'make the unpalatable choice of accepting the damage resulting from the disclosure of information or protecting that information by abandoning that prosecution': Second Reading Speech of the then Attorney-General, Mr Ruddock (Hansard, House of Representatives, 7 December 2004).

23. To address this issue, the ALRC recommended a new statutory regime, placed in a dedicated Act, to govern the use of national security information in civil and criminal proceedings. The Explanatory Memorandum to the *National Security Information (Criminal Proceedings) Bill 2004* explained how it would address the issue:

> The *National Security Information (Criminal Proceedings) Bill 2004* seeks to protect information from disclosure during a proceeding for a Commonwealth offence where the disclosure is likely to prejudice Australia's national security…
>
> The existing rules of evidence and procedure do not provide adequate protection for information that relates to, or the disclosure of which may affect, national security, where that information may be adduced or otherwise disclosed during the course of a federal criminal proceeding.
>
> Prosecutions for espionage, treason, terrorism, and other security-related crimes may require the disclosure of such information to persons who are not security cleared, including members of a jury. As a consequence, the Commonwealth may be faced with a choice between accepting the damage resulting from the disclosure of information or protecting that information by abandoning the prosecution.
>
> The Bill is designed to provide a procedure in cases where information relating to, or the disclosure of which may affect, national security could be introduced during a federal criminal proceeding. The aim of the Bill is to allow this information to be introduced in an edited or summarised form so as to facilitate the prosecution of an offence without prejudicing national security and the rights of the defendant to a fair trial.

24. The NSI Act has addressed these issues and has been used in over 40 prosecutions including *R v Thomas (2005), R v Lodhi (2005), R v Benbrika et al (2008), R v Khazaal (2006), R v Elomar et al (2006), R v Aweys (2010), R v El Sayed at al (2009), R v Al Ahmadzai (2013), and R v Scerba (2015).* The NSI Act has also been used successfully in a small number of civil proceedings including Roberts-Smith v Fairfax Media (2020).

25. The NSI Act has and continues to successfully enable law enforcement to obtain and use information from intelligence agencies to prosecute criminal cases. The availability of the NSI Act increases the willingness of intelligence agencies, including international partners, to agree to the use of national security information in prosecutions.

26. If the NSI Act were repealed the problems which arose in *R v Lappas* could arise again. Given the current threat environment we will see more espionage and foreign interference prosecutions, not less, in future and the NSI Act will be critical in enabling those prosecutions to occur.

## How the NSI Act Operates in Practice and Why it is Still Necessary

27. In addition to addressing the issue that arose in *R v Lappas*, the NSI Act has provided a consistent, transparent and reliable framework through which the courts, with assistance from the parties and the Attorney-General, can manage the disclosure, protection, storage, handling and destruction of national security information in federal civil and criminal proceedings. The key features of the NSI Act are:

a. The NSI Act complements rather than displaces the legislative and common law powers available to a court to manage the protection of national security information. The NSI Act only applies to legal proceedings involving national security information if invoked. The NSI Act is not always invoked in federal criminal and civil proceedings involving national security information. Sometimes, where the issues are straightforward, there is no need to invoke the NSI Act as the court's other powers may be sufficient. In practice, the NSI Act is more likely to be invoked in complex cases where national security information is central to the proceedings and less likely to be invoked where it is tangential.

b. Once invoked, the NSI Act gives the Attorney-General a right to attend and be heard in relation to the disclosure, protection, storage, handling and destruction of national security information in the proceedings (s. 20A, s. 38AA).

c. The prosecutor, defendant or defendant's legal representatives in a criminal proceeding, or the parties and their legal representatives in a civil proceeding, must give notice to the Attorney-General if they know or believe that national security information is likely to be disclosed in the proceedings (s. 24 – s. 25, s. 38D – s. 38E). The notification requirements apply to a range of circumstances including disclosure by the parties, their witnesses and third parties responding to a subpoena. The most important feature of the notification provisions is that they give the Attorney-General an opportunity to engage with relevant subject matter experts and assess whether disclosure of the information would prejudice national security *before* the information is disclosed.

d. If the Attorney-General is notified about a likely disclosure of national security information in the proceeding, or if the Attorney-General expects that such a disclosure will be made, the Attorney-General may issue a non-disclosure certificate describing the information that needs to be

protected and explaining the circumstances in which its disclosure is permitted. While less common in practice, the Attorney-General may also provide the information in a form that is considered suitable for disclosure (for example, a redacted copy of a document, summary of information or statement of facts) (s. 26, s. 38F). Two features should be emphasised:

i. While the non-disclosure certificate is conclusive evidence for part of the criminal trial process that the disclosure of the information is likely to prejudice national security (s. 27), this is the start not the end of the process. The certificate ceases to have effect once the court makes orders under s. 31 of the NSI Act and they are no longer subject to appeal (s. 26(5), s. 38F(6));

ii. The fact that it is the First Law Officer of the Commonwealth, and not the national security agencies whose information may require protection, who issues the non-disclosure certificate is also significant. As First Law Officer, the Attorney-General has responsibilities to ensure the proper administration of law and justice as set out in the Administrative Arrangement Orders and is responsible to both the Parliament and the electorate. Non-disclosure certificates are not issued lightly.

e. Where a non-disclosure certificate is issued, the NSI Act *requires* the court to hold a *closed* hearing (s. 29, s. 38I) to determine whether to make an order (under s. 31) in relation to the disclosure of the information. Hearings in relation to the sensitivity of national security information must take place in closed court to encourage candour because often, the explanation for why national security information is sensitive is more sensitive than the information itself. This was addressed by Justice Whealey in *R v Lodhi* (2006) 163 A Crim R 448:

> … The fact that the s 31 hearing is to be a closed hearing does not place an undue burden given the legitimate aim of such a hearing and the subject matter with which it deals. It is a limited hearing dealing with a limited topic. The closure of the court and the limitations on those who may appear at the closed hearing is likely to engender a more candid and frank discussion about any national security issues; and at the same time re-enforce the safety of sensitive material from unnecessary disclosure at that preliminary point in the proceedings. In that respect, it is not far different from the method in which a public interest immunity claim is dealt with by a court dealing with sensitive material: at [123].

f. At the conclusion of the hearing the court must make an order in relation to the national security information that was subject to the non-disclosure certificate (s. 31, s. 38L) and must give written reasons for its decision (s. 32, s. 38M). The court is able to make orders in relation to who the information can be disclosed to and in what circumstances. The court may order that the information not be disclosed other than in accordance with the Attorney-General's non-disclosure certificate, it may order that the information be disclosed to the world at large despite the Attorney-General's non-disclosure certificate, or it may make another order entirely:

i. If the court allows summaries of information or statements of fact to be disclosed they will only be admissible as evidence of the contents of the document on which they were based if the contents would be admissible (s. 31(3), s38L(3));

ii. In determining what order to make under s. 31 or s. 38L of the NSI Act the court must consider whether disclosure of the information in contravention of the non-disclosure certificate would prejudice national security and whether the order it proposed to make would have a substantial adverse effect on a defendant's right to a fair hearing, including the conduct of his or her defence. In making the decision, the court is required to give the greatest weight to the risk of prejudice to national security;

iii. The court must also have regard to the object of the NSI Act (in s. 3) which is to prevent disclosure of information where the disclosure is likely to prejudice national security, except to the extent that disclosure would seriously interfere in the administration of justice;

iv. For the reasons set out later in this submission, these are appropriate considerations for a court to consider when deciding whether to order the disclosure of national security information contrary to a non-disclosure certificate. To the extent that the NSI Act tips the balance regarding disclosure in favour of national security – it should. The administration of justice is preserved (because the order cannot be made if it would be seriously interfered with) as is a defendant's right to a fair hearing (because the proceedings can be stayed if the court determines that non-disclosure would substantially affect that right).

g. The NSI Act requires the Court, before publishing a record of the closed hearing, or its reasons, to consult with the Attorney-General and the prosecutor who may request that the record be varied to remove information the disclosure of which is likely to prejudice national security. If the court chooses to publish the information anyway, the Attorney-General may request that publication be delayed until any appeal has concluded (s. 29, s. 29A, s. 32 – s. 33; s. 38I, s. 3M - 38N). The court must grant that request.

h. Most importantly, if the Court proposes to make an order disclosing national security information contrary to the certificate of the Attorney-General, the prosecutor in a criminal trial or a party in civil proceedings has the option of obtaining an adjournment to allow them to consider withdrawing the proceeding rather than accept having national security information disclosed in accordance with the orders (s. 36, s. 38P). This is vital, because it enables NIC agencies to confidently assure their sources and partners that their information can be protected in legal proceedings (even if the cost of protection is the inability of the Commonwealth to pursue a civil claim or prosecute an offender).

i. If either party is dissatisfied with the orders made by the Court under s. 31 or s. 38L they have a right of appeal (under s. 37, or s. 38R). The prosecutor and the Attorney-General, or the Attorney-General in a civil proceeding, also have a right to appeal decisions in relation to the publication of information disclosed in the closed hearing (s. 36A, s. 38; s. 38Q, s. 38S).

j. None of the orders made under Part 3 Division 3 or Part 3A Division 3 come into effect until after the order ceases to be subject to appeal and any orders remain in force until they are revoked (s. 34, s. 38O). This ensures that national security information is not disclosed until any contest is resolved and that sensitive national security information continues to be protected once the proceedings are over.

k. If the court decides that the national security information needs to be protected, but that doing so would have a substantial adverse effect on a defendant's right to a fair hearing or on the substantive hearing in a civil proceeding – then the NSI Act enables the proceedings to be stayed (s.19(2), s. 19(4)(5)). Likewise, the prosecutor retains the ability to discontinue a proceeding and will be compelled to do so where the defendant cannot, or can no longer, receive a fair hearing. In civil matters the court is required, before staying proceedings, to consider the extent of any financial loss that a party would suffer as a result of the stay and whether a party had reasonable prospects of obtaining a remedy in the proceeding.

l. Outside of the Attorney-General's non-disclosure certificate process, the NSI Act also gives the parties and the court a range of efficient and flexible options to manage national security interests and minimise any disruption to the proceedings:

    i. The parties and the Attorney-General, at any time during the proceedings, can agree to an arrangement about the disclosure, protection, storage, handling or destruction in the proceedings of national security information. The court can make 'any such order as it considers appropriate' to give effect to the arrangement (s. 22, s. 38B) including a discretion to make no orders at all. Arrangements by consent are the most common and efficient way in which protective orders are made under the NSI Act;

    ii. If the court wishes to make orders in relation to the disclosure, protection, storage, handling or destruction of national security information in the proceeding, it also has a broad discretion to make *'such orders as the court considers appropriate'* provided that the court is satisfied that it is in the interests of national security to make such orders and they are not inconsistent with the NSI Act or Regulation (s. 19(1A), s. 19(3A));

    iii. Part 4 of the NSI Act also establishes a framework through which a party in civil proceedings or a legal representative or someone assisting a legal representative (in civil or criminal proceedings) may be granted a security clearance to access national security information in the proceedings. If the person chooses not to apply for a clearance or is unable to obtain one, they may not be given access to some national security information and may be excluded from closed hearings (under s. 29 and s. 38I). While the legal representatives of parties involved in legal proceedings have rarely been required to obtain security clearances, these provisions are important and should be retained for exceptional cases.

m. The NSI Act also allows for regulations to be made prescribing ways in which national security information that is disclosed in the proceedings must be stored, handled or destroyed and the

ways, and places in which, such information may be accessed and documents or records relating to such information may be prepared (s. 23, s. 38C). The NSI Regulation is a transparent and effective way to address these issues and can avoid the need for extensive procedural orders to be made on a case by case basis.

n. The NSI Act and Regulation not only make complex litigation involving extensive national security information workable, it also enables Australian Government agencies to reassure foreign partners who share their most sensitive intelligence and capabilities with us that they can and will be protected in legal proceedings. In providing such reassurance, intelligence agencies rely heavily on the fact that:

    i. Australia has a specific legislative regime in place to protect national security information from disclosure in legal proceedings. That regime is at least as robust as equivalent legislation overseas (for example the *Classified Information Procedures Act* in the United States) and requires the court, when determining whether to disclose national security information, not only to consider any prejudice that may be caused to national security, but to give the greatest weight to it;

    ii. Any sensitive information provided by our partners will be protected from disclosure: either by an Attorney-General's non-disclosure certificate or court order (breaches of which attract criminal penalties); or if a court is not convinced of the need to protect that information (following a closed hearing in which we can lead evidence) the Commonwealth can either discontinue the proceedings or withdraw/settle a civil claim.

28. One of the key benefits of the NSI Act is that it promotes the early identification and resolution of issues relating to the disclosure and protection of national security information. The broad definition of national security information encourages early notification and engagement between the parties and the Attorney-General. Once notification is given, the Attorney-General and the parties are able to identify the types of national security information that is likely to be disclosed in the proceedings and agree to orders under s. 22 or s. 38B. Where agreement cannot be reached, a hearing will take place and the court will make orders under s. 31 or s. 38L. But for the wide definition of national security information and the mandatory requirements for notices and adjournments, there would be little incentive for a defendant or their legal representatives to engage in early discussions about s. 22 orders. As a result of the NSI Act, information protection issues rarely, if ever, arise for the first time during the trial.

29. While there are other mechanisms available to achieve some of the same outcomes (such as public interest immunity claims, non-publication and suppression orders, or relying on inherent powers to close a court or make pseudonym or screening orders) they are not as broad or flexible as those available under NSI Act. In practice, it can be difficult to rely on these powers without undesirable disruption to the trial (for example, making public interest immunity objections during the questioning of a witness) or unacceptable risk to the information (for

example, the witness answers the question before the objection is heard). They can be more complex, less efficient and provide less certainty, particularly when trials are taking place before judges who may have had limited exposure to the practicalities of managing national security matters. They also, unlike the NSI Act, do not provide adequate protection for national security information until after the orders have been made.

2. Whether the interaction of the protection of national security information and the public adjudication of disputes according to law would better occur if the *NSI Act* were repealed. In particular, whether powers available to courts, in the absence of the *NSI Act*, can more appropriately deal with this interaction than the processes required by the *NSI Act*.

## Delay and Complexity

30. One of the concerns raised about the NSI Act, particularly in the recent case of *R v Collaery,* was that it is complex and can cause delay.

31. The reality is that managing the disclosure of large volumes of national security information in legal proceedings and striking an appropriate balance between competing public interests is a complex and time-consuming exercise irrespective of whether the NSI Act is invoked, or not.

32. *R v Collaery* was certainly a lengthy and complex matter. Mr Collaery was charged with conspiring to disclose classified information to a foreign government and with disclosing classified information contrary to s. 39 of the ISA. He contested applications by the Commonwealth to protect from public disclosure certain classified information contained within the prosecution brief of evidence and he issued subpoenas to Commonwealth agencies to compel the production of additional classified information. The litigation was time consuming and complex with extensive evidence adduced by both parties, some disruptions by the COVID-19 pandemic, and an appeal. However, this would have been a time consuming and complex exercise because of these factors and the competing public interests irrespective of whether the NSI Act had been invoked.

33. In legal matters where national security information is to be disclosed, arrangements must be put in place for practical aspects such as the storage and handling of classified information, the secure conduct and transcription of hearings, the redaction of classified documents and transcripts to be made available to the public, and the protection of identities. This is never a simple exercise. The NSI Act can streamline this process, particularly where the parties and the Attorney-General can agree to an arrangement under s. 22 or s. 38B of the NSI Act. Even if agreement cannot be reached on all aspects, it provides a clear and flexible framework through which appropriate orders can be made. Even in the Collaery case, there were significant matters which were able to be resolved through the use of s. 22 orders.

## Amendments

34. While we do not believe that the NSI Act is slow or complex compared to the alternative processes available to protect national security information in legal proceedings, there are four areas in which improvements could be made:

a. Firstly, **the NSI Regulation should be reviewed** to ensure that it remains fit for purpose. The current Regulation was made almost a decade ago (in 2015) and provides basic requirements in relation to the disclosure, protection, storage, handling and destruction of national security information in proceedings. In recent cases, more comprehensive orders have been required under s. 22 and s. 38B on the NSI Act. If the Regulation were updated to include some of the more common orders now made routinely under s. 22 and s. 38B, consent orders would be required less frequently on uncontroversial matters which would speed up the litigation process. Updating the Regulation would also lead to greater transparency through easy public access to the Regulation, efficiency and consistency compared to the need for s. 22 and s. 38B orders in each case.

b. Secondly, the **NSI Act could be amended so that it can be invoked to provide protections in anticipation of legal proceedings** to facilitate negotiation between parties to narrow or resolve disputes before the commencement of any proceedings. As currently drafted, the NSI Act can only be invoked once proceedings have commenced. In some cases, for example where a civil claim has been foreshadowed and the parties wish to engage in an informal preliminary discovery or an early mediation process, it would be helpful for the Attorney-General to be able to invoke the NSI Act and issue a non-disclosure certificate prior to the commencement of proceedings. This would enable intelligence agencies to disclose information earlier (relying on the fact that the criminal penalties under s. 43, s. 45A, s. 46D and 46FA of the NSI Act would prevent further disclosure) and, where appropriate, settle suitable matters prior to the commencement of legal proceedings.

c. Thirdly, the NSI Act should be amended to **restrict appeals under Part 3 Division 4 and Part 3A Division 4 of the NSI Act to questions of law**. As the NSI Act does not specify the form of an appeal, s. 79(1) of the *Judiciary Act 1903* mandates that the procedure of whichever State or Territory court is exercising federal jurisdiction will apply. In the ACT, for example, this is an appeal by way of re-hearing. Given the inherent complexity in evaluating national security risks (the expertise for which sits within the executive arm of Government – see *Alister v R* (1984) 154 CLR 404 at 435) and the balancing exercise required under s. 31 of the NSI Act, this task should be carried out by the trial judge who has heard the evidence, not by an appeal court. Limiting appeals to questions of law would ensure consistency in all NSI Act appeals (rather than applying the procedure of whichever State or Territory the case is in), minimise the likelihood and complexity of any appeal and expedite the trial.

d. Finally, we recommend that consideration be given to the feasibility of establishing **a National Security Division of the Federal Court, or equivalent in relevant State and Territory**

**jurisdictions**, to hear cases in which the NSI Act has been invoked (or at least those parts of the proceedings where decisions need to be made regarding the protection or disclosure of national security information, as occurs in the United States under CIPA). This would enable:

i. Appropriate infrastructure for the secure communication and the storage, handling and destruction of national security information to be put in place in advance of proceedings. This would save a lot of time and inconvenience for the court and also promote better security (for example, by avoiding or reducing the need to safehand classified material). It may not be feasible to establish physical facilities in a wide range of courts, but it may be useful and efficient for a court equipped with such a facility to make it available to other courts to sit in when they need secure facilities;

ii. Facilities could be accredited in advance to store Top Secret codeword material. An audio secure courtroom with secure transcription facilities could be available for closed court hearings. A secure IT network could be provided so that judges and court staff do not need to rely on stand-alone laptops and printers. The courtroom could be designed to facilitate the covert entry or screening of witnesses whose identities need to be protected. This would save time and, in the long run money, and would help to mitigate some of the more significant risks inherent with national security litigation;

iii. By establishing a National Security Division, a pool of judges and well-trained security cleared court staff could be identified by the court to develop expertise in national security litigation, including the operation of the NSI Act and more general familiarity with the practicalities of handling classified information. Where appropriate, and consistent with the independence of the judiciary, they could also be provided with briefings regarding the contemporary threat environment and any risks posed by foreign intelligence services to the judiciary. Court staff could be provided with suitable training and, if appropriate, security clearances. This would address the recurrent challenge of running national security litigation in State and Territory Courts that have had no or limited exposure to the practicalities of storage and handling of national security information and/or do not have the facilities to conduct secure hearings.

**3.** If the *NSI Act* is to be retained; whether, in federal criminal proceedings the balancing of factors by the Court required by section 31(7) and the requirement of section 31(8) that the Court give greatest weight to the factor provided for in section 31(7)(a), is appropriate. Whether the equivalent provisions in respect of civil proceedings in section 38L are appropriate.

35. The balancing exercise in s. 31(7)(8) and s. 38L(7)(8) is appropriate and should be retained.

36. In deciding whether to order the disclosure of national security information (contrary to a certificate issued by the Attorney-General on advice from intelligence professionals) the court *should* consider whether:

a. having regard to the Attorney-General's certificate, there would be a risk of prejudice to national security if the information were disclosed or the witness were called;

b. the order it proposes would have a *substantial* adverse effect on the defendant's right to receive a fair hearing in a criminal proceeding or on the substantive hearing in a civil proceeding; and

c. any other matter the court considers relevant.

37. When weighing up public interest considerations the court *should* give the greatest weight to whether there would be a risk of prejudice to national security if information were disclosed '*in contravention of the Attorney-General's non-disclosure certificate*'.

38. The reference to contravening the Attorney-General's non-disclosure certificate is important. The NSI Act does not simply require that greater weight be given to national security relative to other public interest considerations. It says that the court should give the greatest weight to the risk of prejudice to national security *if* information were to be disclosed in contravention of the Attorney-General's non-disclosure certificate. This recognises the significance of a non-disclosure certificate, including that the Attorney-General, who is the elected official uniquely well-placed to assess national security risks and the proper requirements of the administration of justice has considered those matters and assessed that the information should not be disclosed.

39. The Attorney-General's assessment of what is in the public interest should not be set aside lightly because:

a. It is inherently difficult for a court to assess the harm that may be caused by the disclosure of national security information. As the House of Lords acknowledged in *SSHD v Rehman* [2003] 1 AC 153 it is the executive arm of Government that is 'undoubtedly in the best position to judge what national security requires' even if its decision is open to review;

b. As the High Court said in *Alister v R* (1984) 154 CLR 404, national security is a public interest 'of special importance'. 'Questions of national security naturally raise issues of great importance, issues which will seldom be wholly within the competence of the court to evaluate'. As such, while it may not be conclusive, 'very considerable weight must attach to the view of what national security requires as expressed by the responsible Minister';

c. It is the executive arm of the Government, not the judiciary, that is tasked with protecting national security so the court must be 'more than ordinarily cautious in requiring the production of security documents…' *Alister v R at* 439;

d. Requiring the disclosure of national security information contrary to an Attorney-General's certificate or failing to give sufficient weight to the risk of prejudice to national security, could undermine the trust and confidence that our partners and allies have in the Australian judicial system and may discourage future disclosures, depriving the court and the parties of the best evidence available;

e. The consequences of disclosing national security information in contravention of the Attorney-General's non-disclosure certificate, could be catastrophic (and may cause the very damage that the NSI Act is intended to prevent).

40. Concerns that the framework set out in the NSI Act for managing the disclosure of national security information might be unconstitutional and that the requirement to give the greatest weight to national security risked compromising the right of a defendant to a fair trial were addressed by the NSW Court of Criminal Appeal in *R v Lodhi* (2006) 168 A Crim R 448 and *Lodhi v The Queen* (2007) 179 A Crim R 470. Most recently, *R v Collaery (No 7)* (2020) 283 A Crim R 524, Mossop J referred to Spigelman CJ's judgment in the *Lodhi* appeal relating to ss 31(7) and (8) and stated at [41]-[43]:

> Section 31(8) requires that the court "must give greatest weight" to the consideration referred to in s. 31(7)(a). That does not mean that the consideration will necessarily predominate over other considerations. *In Lodhi v The Queen* at [36], Spigelman CJ quoted with approval Whealy J's explanation of the operation of s 31(8) as follows:
>
> > The mere fact that the legislation states that more weight, that is the greater weight, is to be given to one factor over another does not mean that the other factor is to be disregarded. The use of the expression "greatest weight" appears to be grammatically correct since the legislation is contemplating three (or more) considerations. Nor do I consider that the discretion is an exercise that, as was argued, will almost inevitably lead to one result namely, prevention of disclosure. Mr Boulten SC described it as "filling in the dots". I cannot agree with this description. Read fairly, it seems to me that the legislation does no more than to give the Court guidance as to the comparative weight it is to give one factor when considering it alongside a number of others. Yet the discretion remains intact and, particularly for the reasons I have outlined, it seems to me that there

> is no warrant for supposing other than that, in a proper case, the Court will order disclosure or a form of disclosure other than that preferred by the Attorney-General. The legislation does not intrude upon the customary vigilance of the trial judge in a criminal trial. One of the court's tasks is to ensure that the accused is not dealt with unfairly. This has extended traditionally into the area of public interest immunity claims. I see no reason why the same degree of vigilance, perhaps even at a higher level, would not apply to the Court's scrutiny of the Attorney's certificate in a s 31 hearing.

As Spigelman CJ went on to explain (at [38]), this interpretation means that even if there is a significant risk of prejudice to national security, the giving of that consideration greater weight will not necessarily lead to non-disclosure if the adverse effect on the defendant's right to receive a fair hearing is substantial enough.

The exercise required by s. 31(7) and (8) involves comparison between conflicting interests that are incommensurable: *Lodhi v The Queen* at [40]. Section 31(8) does tilt the balance or "put a thumb on the scales" but this "is perfectly consistent with the traditional judicial decision-making process": *Lodhi v The Queen* at [41].

41. It is also important to remember that the balancing exercise in s. 31(7)(8) and s. 38L(7)(8) does not occur in isolation, but within the context of a broader scheme that ensures that decisions made under s. 31 of the NSI Act do not seriously interfere with the administration of justice (s. 3(2)) or impinge upon a defendant's right to a fair trial. The right to a fair trial is given primacy by s. 19(2) of the NSI Act which enables a court to stay a proceeding if the decision to protect national security information would have a substantial adverse effect on a defendant's right to receive a fair hearing.

42. In practice, the outcome of the balancing exercise under s. 31 and s. 38L has not, as far as we are aware, prevented a Court from acting where it is concerned the application of the 'greatest weight' requirement in s. 31(8) or s. 38L(8) might compromise the administration of justice. In practice, where courts have been satisfied that national security considerations outweigh competing interests they have made orders protecting the information. Where they have not been so satisfied, they have ordered disclosure.

43. These sections also send an important message to foreign intelligence services who might be minded to target legal proceedings, and to our allies and intelligence partners who may be reluctant to share national security information if it cannot be protected in legal proceedings. The message is that the Australian Government (and once legal proceedings are on foot, the courts) take the protection of national security information very seriously (to the point where national security considerations are not just taken into account but given '*the greatest weight*') and are unlikely to disclose national security information contrary to an Attorney-General's certificate unless withholding the information would have a *substantial* adverse effect on a defendant's right to a fair hearing or would have a substantial adverse effect on the substantive hearing. This is an important message, particularly in the current threat environment.

44. Revoking s. 31(8) and s. 38L(8) or altering the balancing exercise in favour of disclosure risks sending the *opposite* message: namely that the Australian legal system is becoming a more attractive environment in which to collect intelligence; that the need to protect national security will no longer be given the greatest weight in legal proceedings; and that sensitive national security information may be disclosed even where protecting it would not have substantially affected a defendant's right to a fair trial or the substantive hearing in a civil proceeding. This is not the right message to be sending to our international partners, or to hostile foreign intelligence services in the current threat environment.

**4.** If the *NSI Act* is to be retained; whether the definition of the key integer of "national security information" in the *NSI Act* is too broad, and in this respect its relation to "matters of state" in section 130 of the *Evidence Acts*.

## Definition of National Security Information

45. National security information is defined under the NSI Act as information 'that relates to national security' or the 'disclosure of which may affect national security'. National security is defined as meaning 'Australia's defence, security, international relations or law enforcement interests'. These categories reflect a number of well-established categories of public interest immunity and allow flexibility to meet a complex and changing threat environment.

46. In Australia's First National Security Statement to the Australian Parliament, the then Prime Minister, the Hon Kevin Rudd MP, noted that the 'increasingly fluid' security environment was characterised by a complex and dynamic mix of continuing and emerging challenges and opportunities. He stated that, while our national security interests remain constant, 'the concept of national security needs to be capable of embracing and responding to the more complex and interconnected operating environment that we will face for the future'. Mr Rudd referred to national security in broad terms consist with its NSI Act definition. He stated that the Australian government was focussing on 'clear and enduring security interests that transcend the scope of state and territory jurisdictional responsibilities' including:

- maintaining Australia's territorial and border integrity;
- promoting Australia's political sovereignty;
- preserving Australia's cohesive and resilient society and the long-term strengths of our economy;
- protecting Australians and Australian interests both at home and abroad; and
- promoting an international environment, particularly in the Asia-Pacific region, that is stable, peaceful and prosperous, together with a global rules-based order which enhances Australia's national interests.

47. While the definition of 'national security information' is broad, it *must be* for the NSI Act to work effectively. This is because the term is a trigger for the notification obligations described earlier in this submission. It is appropriate to set this trigger broadly as parties to the proceedings are not subject matter experts, are not well placed to assess national security risks and therefore should be required to err on the side of notification.

48. This is an invaluable process and in practice, the discussion about the sensitivity of information likely to be disclosed in the proceedings is rarely confined to individual documents. Instead, notification leads to discussions between the parties and the Attorney-General about the types of national security information that will be disclosed in the proceedings and how it should be managed. This can result in consent orders being made under s. 22 or s. 38B, or there being a contested hearing on the issue if the parties and the Attorney-General disagree.

49. The mere fact that information falls within the broad definition of 'national security information' does not mean that it will be restricted in the proceedings or withheld from the public. Often national security information can be disclosed in confidence to the parties in the proceeding, or to the world at large. Even when the parties and the Attorney-General agree to an arrangement about the disclosure, protection, storage, handling or destruction of national security information, the Court must still be satisfied that the orders are 'appropriate' before giving effect to the arrangement. Where the parties disagree, a contested hearing takes place and the Court will determine for itself, weighing up the competing public interests, what orders should be made. If the parties are unhappy with those orders, then they have a right of appeal.

50. Adopting a narrower definition of 'national security information' would undermine the object of the NSI Act by limiting the circumstances in which notification is given and allowing parties who may be ill-equipped to assess national security risk (and may be on trial for having disclosed classified documents) to determine for themselves what harm, if any, would result from potential disclosures. It would create a significant risk that sensitive national security information will be disclosed in proceedings prior to any engagement with the Attorney-General or experts best placed to identify/assess the risks of such disclosure. Once disclosed, the information cannot be un-disclosed and the damage caused to national security cannot be undone.

## Definition of Security

51. Given that the INSLM is considering whether, or not, the definition of 'national security' in s. 8 of the NSI Act is too broad, we recommend that the INSLM also consider the related definition of 'security' in s. 9.

52. As currently drafted, 'security' in s. 9 of the NSI Act is given the same meaning as in the ASIO Act. If the definition of 'national security information' is altered then consideration should also be given to expressly including in it 'operationally sensitive information' as defined in Part 1A of Schedule 1 in the ISA, as well as the identities of ASIO employees or affiliates and ASIS staff members or agents. The need to afford special protection to this type of national security information is specifically recognised in the ASIO Act and ISA. It would seem appropriate to expressly recognise these categories of national security information in the NSI Act.

## 5. If the *NSI Act* is to be retained; whether the *NSI Act* should expressly provide for appointment of a special advocate, and if so, how, when and on what terms.

53. In the past, there has been little need for special advocates in civil and criminal proceedings (other than control order proceedings) in which the NSI Act has been invoked. This is because the NSI Act has rarely been used to withhold information from parties to legal proceedings and their legal representatives and, where information has been withheld on public interest immunity grounds, the courts have not required the assistance of a special advocate.

54. The ability of the court to appoint a special advocate in NSI Act matters was considered by the New South Wales Court of Appeal in *R v Lodhi* [2006] NSWSC 586. In that case Justice Whealey found that the court did not need a statutory basis to appoint a special advocate and that the provisions of the NSI Act were not inconsistent with the appointment of one. He noted, however, that while the court had the power to appoint a special advocate 'it should do so only if the Court is satisfied that no other course will meet the overriding requirements of fairness to the defendant'. As the House of Lords stated in *R v H; R v C* (2004) 2 AC 134 'such appointments will always be exceptional, never automatic; a course of last and never first resort'.

55. It might be appropriate for the court to appoint a special advocate in circumstances where a court thinks it is appropriate to admit national security information as evidence in the proceedings, but not make it available to the other party or their legal representatives. This could include: where the Attorney-General seeks to lead court only evidence in a s. 27 hearing in support of s. 31 orders (as occurred in *R v Collaery*); where a prosecutor seeks to use redacted documents or summaries of information as evidence and the original information is not made available to the defendant or his legal representatives; or if a party's legal representative is excluded from closed court proceedings because they do not have an appropriate security clearance.

56. As *R v Collaery* demonstrates express provision in the NSI Act is not required for the Court to appoint a special advocate in an NSI Act matter. Nevertheless, if express provision were to be included in the NSI Act it would provide an opportunity for the Act to address several issues which might be expected to arise such as:

a. Will the court retain its discretion to appoint (or decline to appoint) a special advocate depending on the circumstances of a case? It should;

b. If special advocates are to be appointed under the NSI Act, when should they be appointed? They should only be appointed to test evidence in the proceedings that the other party is unable to review in its unredacted form. Special advocates should not be appointed under the NSI Act to assist a court in determining public interest immunity claims. This would be unnecessary,

inconsistent with the common law, would delay and increase the cost of proceedings and create a disincentive for invoking the NSI Act;

c. What role will the special advocate play? The role should be essentially as a contradictor to test the evidence that is not available to that party, rather than to protect and advance that party's interests generally, for example by adducing evidence on unrelated issues or contributing to the case in a broader way that overlaps tasks that the party or their representative is already placed to do.

d. How will the special advocate be identified and appointed? A minimum qualification should be that the special advocate holds a security clearance commensurate with the classification of the material concerned. It might be appropriate for the Attorney-General's Department to maintain a list of security cleared counsel and to ensure that there is a sufficiently large pool of cleared counsel available. The court should have final say over who is appointed and should be satisfied that the special advocate will have the experience and expertise to properly assist the court in performing the role.

e. Will special advocates have solicitors assisting to support them? If so, who and how many and how should they be selected? Solicitors assisting should also be security cleared and the size of the solicitor team should be determined according to what is reasonably necessary for the circumstances of the case.

f. Who will assess the reasonableness of the special advocates legal fees? Will those fees be at the Commonwealth Government rate approved under the Legal Services Directions? Appropriate arrangements will need to be in place to properly oversight the expenditure of public funds, without unfairly compromising the confidentiality of the special advocate's work. There will need to be appropriate separation between the official ensuring the costs have been reasonably incurred and other officials involved in the substantive proceedings.

g. There will also need to be clear arrangements relating to how special advocates engage with their 'client' and what information they can and cannot share with them. Usually, special advocates are prohibited from speaking to their 'client' after they have had access to protected information to avoid inadvertent disclosure.

h. The Act should also include appropriate offence provisions to ensure that special advocates do not disclose national security information to those who are not authorised to see it (particularly their 'client') or use that information for other purposes, or in other legal proceedings.

## 6. If the *NSI Act* is to be retained; whether the processes of the *NSI Act* should be expanded to apply not only to federal criminal proceedings and civil proceedings as currently defined.

57. For the reasons set out above, the NSI Act provides a transparent and reliable framework through which to manage the disclosure of national security information in legal proceedings. For that reason, we would support legislative amendment to make the NSI Act, or similar protections, more widely available, including in state and territory criminal proceedings and coronial inquiries.

58. That said, in our experience the types of matters where national security information is central, rather than peripheral, to a case are most likely to arise in the Federal jurisdiction. As such, while there may be some benefit in extending NSI protections they may not outweigh the significant challenges such change is likely to present. The 2019 Comprehensive Review of the Legal Framework of the National Intelligence Community ('the Richardson Review') considered the limited application of the NSI Act and the extent to which it should be extended to state and territory criminal proceedings, coronial inquiries or to all courts and Tribunals. The Review did not support the extension of the NSI Act, noting that the associated reforms would be 'significant' and that different considerations may apply to other types of legal proceedings.

59. Further, we do not believe that there is a need, or that it would be appropriate, to extend the NSI Act to the administrative review of Government decision making (for example in the Commonwealth Administrative Appeals Tribunal or its successor) where there is already an appropriate and robust mechanism for protecting national security information and different public interest considerations and more extensive disclosure requirements may apply.

60. We also understand that the protection of national security information in administrative review proceedings is already being considered by the Government in the context of its proposed establishment of a new federal administrative review body.

**7.** If the *NSI Act* is to be retained; the adequacy or appropriateness of the penalties under Part 5 of the *NSI Act*, including having regard to the maximum penalties provided under Part 6 of the *Intelligence Services Act 2001* (Cth), *Part 4 of the Office of National Intelligence Act 2018* (Cth) and Part 3 of the *Australian Security Intelligence Organisation Act* 1979 (Cth).

61. There is a lack of parity between the penalties imposed under the NSI Act and penalties imposed for equivalent offending under the ASIO Act, the ISA, the ONI Act and the Criminal Code. Despite the consequences of disclosure being similar, or in some cases even worse, and the conduct at least as serious, the penalties imposed under the NSI Act are lower than all comparable secrecy offences and are inadequate to deter or punish worst case offending, including repeat offending.

62. Commonwealth criminal law policy, as set out in the *Guide on Framing Commonwealth Offences*, states that 'a maximum penalty should aim to provide an effective deterrent to the commission of the offence, and should reflect the seriousness of the offence within the relevant legislative scheme'. A higher maximum penalty will be justified where there are strong incentives to commit the offence, or where the consequences of the commission of the offence are particularly dangerous or damaging. The penalty should also be consistent with penalties for existing offences of a similar kind or of a similar seriousness.

63. A detailed analysis of existing offences under the ISA, the ONI Act, the ASIO Act and the Criminal Code and why they are of a similar kind and similar seriousness to the NSI Act offences is set out in **Attachment 1** to this submission.

64. For the reasons set out in **Attachment 1** and below, the maximum penalties under Part 5 of the NSI Act should be brought in line with Part 6 of the ISA, Part 4 of the ONI Act, Part 3 of the ASIO Act and s. 122.1 and s. 122.2 of the Criminal Code:

- The penalty for breaching s. 40 – 45, s. 46, s. 46A – s. 46F and s. 46G of the NSI Act should be increased from 2 years to 10 years' imprisonment consistent with s. 39 – s. 40B and s. 41 of the ISA, s. 42 of the ONI Act, s. 18 and s. 92 of the ASIO Act and the aggravated offences under s. 122.1(1) and s. 122.2(1) of the Criminal Code;
- The penalties for breaching s. 45A and s. 46FA of the NSI Act should be increased from 6 months to 3 – 5 years' imprisonment consistent with s. 40C – 40M of the ISA, s. 44 of the ONI Act, s. 18A – s. 18B of the ASIO Act and the aggravated offences under s. 122.1(2)(3)(4) and s. 122.2(2)(3)(4) of the Criminal Code.

65. Bringing the maximum penalties under Part 5 of the NSI Act in line with equivalent penalties in the ISA, ONI Act, ASIO Act and Criminal Code is consistent with recommendations made in 2019 by the Richardson Review. The Review found that 'the harm that could flow from the disclosure

of information in breach of the offences in the NSI Act is equal to the harm that could flow from the disclosure of the same information in breach of the secrecy offences in the ISA and Criminal Code'. The Review accepted that the penalties under Part 5 of the NSI Act 'are too low, and without amendment, are unlikely to be effective in deterring and punishing disclosure of national security information'. The Review also found that it would be possible to increase the maximum penalties for breaching the NSI Act to 10 years consistent with the ISA, or up to 10 years consistent with the Criminal Code.

## Seriousness of the Offending and Adequacy of Current Penalties

66. Part 5 of the NSI Act creates a range of offences to ensure compliance with the Act. Each of the offences is objectively serious because of the harm that may result from the disclosure of national security information. The offences are also serious because of the conduct involved. All but two of the offences involve a person either:

- disclosing what they know to be national security information (or taking action that could have that effect) in circumstances where this is likely to prejudice national security (s. 40 – s. 42, s. 46A – s. 46C, s. 46 and s. 46FA);
- disclosing information in contravention of the Attorney-General's non-disclosure certificate (s. 43, s. 46D); or
- intentionally breaching a court order (s. 45, s. 46F).

67. The two less serious offences (in terms of conduct, but not necessarily consequence) involve failing to store, handle or destroy national security information in accordance with the NSI Regulation in circumstances where this is likely to prejudice national security (s. 45A, s. 46FA).

68. Despite their seriousness, the most serious NSI offences only attract a maximum penalty of up to two years' imprisonment. A breach of the Regulation that is considered likely to prejudice national security attracts a maximum penalty of up to six months' imprisonment.

69. The maximum two-year penalty for breaching the more serious offence provisions in the NSI Act was initially on par with equivalent provisions in the *ASIO Act* (s. 18) and the ISA (s. 39 – s. 40).

70. In 2014, the Commonwealth increased the penalties for unlawfully disclosing classified information under the ASIO Act and the ISA from a maximum of two years, to ten years' imprisonment. The rationale for increasing the penalties (which we submit applies equally to the NSI Act) was addressed by the then Attorney-General, the Honourable George Brandis QC, in his second reading speech. He said:

> In addition, the Bill introduces new maximum penalties of 10 years' imprisonment for existing offences involving unauthorised communication of intelligence-related information, *which at two*

> *years' imprisonment are disproportionately low. The higher maximum penalties better reflect the gravity of such wrongdoing by persons to whom this information is entrusted* (emphasis added).

71. The Explanatory Memorandum to the *National Security Legislation Amendment Act (No. 1) 2014*, explained the rationale for increasing the maximum penalty for breaching s. 18(2) of the ASIO Act as follows:

> 678. This measure will ensure that the penalty applying to subsection 18(2) is proportionate to the gravity of the wrongdoing targeted by the offence. As the existing maximum penalty of two years' imprisonment was included in the ASIO Act as originally enacted in 1979, revision is appropriate to ensure its adequacy in the contemporary security environment.
>
> 679. Recent domestic and international incidents involving the unauthorised communication of security intelligence-related information illustrate that *the existing maximum penalty of two years' imprisonment does not accurately reflect the risk of serious harm to intelligence and security interests that is occasioned by such behaviour. Such risks include jeopardising extant intelligence-gathering operations (including the lives or safety of informants and undercover operatives) or investigations or prosecutions reliant upon intelligence information. The intentional unauthorised communication of intelligence information also risks compromising Australia's intelligence-gathering capabilities by undermining relationships of trust and confidence with foreign intelligence partners and human sources* (emphasis added).

72. The Memorandum also explained the rationale for increasing the penalties under Part 6 Division 1 of the ISA for the unlawful communication of ASIS, AGO, ASD and DIO information as follows:

> 794. …The increase in maximum penalty [from 2 years imprisonment] is aligned with that in relation to the corresponding unauthorised communication of information offence in subsection 18(2) of the ASIO Act.
>
> 795. For the reasons set out above in relation to subsection 18(2) of the ASIO Act, this increase in maximum penalty is *necessary to reflect the gravity of the wrongdoing inherent in the unauthorised communication of intelligence-related information, including the significant risk of harm to Australia's national security that such conduct presents.*

73. There are also several secrecy offences under s122.1 and s. 122.2 of the *Criminal Code Act 1995* which are similar in nature to those in the NSI Act. These offences were added into the Criminal Code in 2018 to replace s. 70 and 79 of the *Crimes Act 1914* which were described, at that time, by the Honourable Simon Birmingham in his Second Reading Speech as *'outdated, ineffective and lack[ing] appropriately serious penalties'*.

74. In considering the current 2-year penalty under the NSI Act and whether it is adequate it is important to bear in mind that the penalty imposed under the legislation is the *maximum penalty* aimed to deter *worst case offending*. Worst case offending under the NSI Act might, for example, involve the deliberate disclosure of national security information contrary to a non-disclosure

certificate or court order where the discloser knows the sensitivity of the information and harm from disclosing leading to:

a. the identification of and harm (possibly fatal) to Australian intelligence officers and/or their sources (either domestically, or overseas);

b. the compromise of a counter-terrorism operation leading to a successful terrorist attack in Australia or on Australian interests overseas or the enablement of espionage or foreign interference against Australian interests;

c. the compromise of Australia's AUKUS nuclear submarine development, or other capabilities being acquired as part of Australia's 2023 Defence Strategic Review putting Australia and its allies at grave risk in any future military conflict;

d. the break down or suspension of intelligence sharing arrangements with our foreign partners, on which we rely heavily to identify potential threats to our national security, because they conclude we are unable to protect their intelligence; or

e. substantial damage to Australia's international relations, including undermining our global standing, or key partnerships in the region.

75. Two years' imprisonment for offending of this nature is grossly inadequate. It is inequitable and defies common sense that a person could face up to life imprisonment under Division 91 of the Criminal Code, or 10 years' imprisonment under the ISA, ONI Act or ASIO Act, for disclosing national security information; whereas another person entrusted with exactly the same information during the first person's trial can wilfully disclose it and face no more than 2 years' imprisonment (or six months if the information is compromised through non-compliance with the NSI Regulation). This would be so even where the latter conduct occurred in a high-risk environment and the discloser knew the sensitivity of the information and the fact that disclosure was prohibited.

## Recklessness Offences Under s. 45 and s. 46F of the NSI Act

76. Sections 45 and s. 46F of the NSI Act create offences in relation to *intentionally* contravention of a court order. New offences should be created for *recklessly* contravening a court order. Those new offences should be punishable by up to 2 years' imprisonment.

77. The proposal to introduce these offences into the NSI Act was considered by the Richardson Review. The Review agreed that there was a role for such offences, and possibly other offences under Part 5 of the NSI Act, carrying recklessness as a fault element. The Review recommended that Part 5 offences should be reviewed and redrafted to include a tiered range of penalties commensurate with the fault element specified.

## 8. If the *NSI Act* is to be retained; the adequacy or appropriateness of the protections and disclosure regime in the *National Security Information (Criminal and Civil Proceedings) Regulation 2015* (Cth).

78. As stated earlier in our submission, the NSI Regulation should be updated to include orders now routinely made under s. 22 and s. 38B of the NSI Act. This will ensure greater transparency, minimise delay and make the parties less reliant on consent orders. Some of the orders routinely made in NSI Act matters, which for example are not covered by the Regulation, include the requirement that:

a. national security information only be photocopied by approved people on approved equipment;

b. certain electronic devices be excluded from approved areas, including closed court hearings;

c. national security information only be discussed with approved people in approved areas; and

d. closed court hearings only be transcribed by an approved provider, who holds an appropriate security clearance, using approved equipment.

79. Consideration should also be given to amending s. 23 and s. 38C of the NSI Act to allow a broader range of matters routinely covered by s. 22 and s. 38B orders to be included in the Regulation. Sections 23 and s. 38C are narrower than s. 22 and s. 38B and may not allow, for example, the Regulation to prescribe the requirements set out in b. and c. above.

# Annexure 1: Comparison Between NSI Act, ISA, ONI Act, ASIO Act and Criminal Code Offences

## Disclosure Offences

1. The most appropriate comparators, when considering a suitable penalty for breaching s. 40 – 45, s. 46, s. 46A – s. 46F and s. 46G of the NSI Act are s. 39 – s. 40B and s. 41 of the ISA, s. 42 and s. 44 of the ONI Act and s. 18 and s. 92 of the ASIO Act. Broadly speaking:

    a. Section 39 - 40B of the ISA, s. 42 of the ONI Act and s. 18(2) of the ASIO Act seek to protect information that was acquired or prepared by ASIS, AGO, ASD, DIO, ONI or ASIO in connection with their functions or relates to the performance by those agencies of their functions. They make it an offence, punishable by 10 years imprisonment, *for a staff member, contractor or agent/affiliate of an intelligence agency* to communicate such information (other than in approved circumstances);

    b. Section 41 of the ISA and s. 92 of the ASIO Act seek to protect the identity of ASIS and ASIO staff members and agents by making it an offence, also punishable by 10 years' imprisonment, for *anyone* to disclose information through which they could be identified as a staff member or agent.

2. The ISA, ONI Act and ASIO Act communication offences provide a good benchmark against which the NSI Act communication offence penalties can be assessed. In both cases:

    a. the information that the legislation is seeking to protect is national security information, including information about the identities of ASIS/ASIO staff members and their agents and information acquired by intelligence agencies in connection with their functions or relating to the performance by intelligence agencies of their functions;

    b. the discloser knows that it is national security information and that they are expected to protect it either because they have been notified of this (under the NSI Act) or because they are an employee, staff member, agent or contractor of an intelligence agency (under the ISA, ONI Act and ASIO Act);

    c. the discloser is entrusted with the information, either as a party to legal proceedings or in a professional capacity: either as a legal professional (barrister/solicitor) or Government employee/contractor (court staff/prosecutor/transcriber) under the NSI Act; or as an employee, staff member, agent or contractor of an intelligence agency (under the ISA, ONI Act and ASIO Act);

    d. the discloser typically will have been (or under the NSI Act would be during the proceedings) briefed about the sensitivity of the information and how it must be protected and provided with secure facilities for the storage and handling of national security information;

e. the volume and/or sensitivity of national security information that the discloser will have access to in their professional capacity is significant either as a participant in legal proceedings (under the NSI Act) or as an employee, staff member, agent or contractor of an intelligence agency (under the ISA, ONI Act or ASIO Act); and

f. the consequences of unlawful disclosure are identical. In fact, some of the NSI offences are arguably more serious compared to their ISA, ONI Act and ASIO Act equivalents as the prosecutor is required to prove under the NSI Act not just that the information was of a particular character, but that its disclosure was likely to prejudice national security (this is not the case with the ISA/ONI Act/ASIO Act offences).

3. Other comparable offences in the Criminal Code are s. 122.1(1) and s. 122.1(2). They make it an offence punishable by imprisonment for 7 years (or 10 years if it is an aggravated offence under 122.3 – see below) to:

- *communicate* 'inherently harmful' information which includes classified information as well as information that was obtained, or made on behalf of, an intelligence agency in connection with the agency's functions (122.1(1)); or
- communicate *any* information (whether or not it is inherently harmful) if the communication causes harm, or is likely to cause harm, to Australia's interests (122.2(1)).

4. Section 122.1(1) and s. 122.2(1) apply to people who are given access to national security information by virtue of them being a Commonwealth officer or engaged to perform work for a Commonwealth entity. For the reasons set out above (in a – f above), these offences also provide a reasonable benchmark against which the NSI Act communication offence penalties can be assessed.

## Storage and Handling Offences

5. The most appropriate comparator, when considering a suitable penalty for breaching s. 45A and s. 46FA of the NSI Act are s. 40C – 40M of the ISA, s. 44 of the ONI Act and s. 18A – s. 18B of the ASIO Act. Broadly speaking:

a. Section 40C – 40M of the ISA, s. 44 of the ONI Act and s 18A and s. 18B of the ASIO Act seek to prevent the unauthorised copying, transcribing, retaining, removing, dealing or recording of information acquired or prepared by ASIS, AGO, ASD, DIO, ONI or ASIO in connection with their functions or which relate to the performance by those agencies of their functions. Staff members, contractors, agent/affiliates of an intelligence agency who breach those requirements may be imprisoned for up to 3 years.

6. The ISA, ONI Act and ASIO Act storage and handling offences provide a good benchmark against which non-compliance with the NSI Regulation can be assessed. In both cases:

a. the making of unauthorised records (under the ISA, ONI Act and ASIO Act) or the failure to properly, store, handle or destroy such records created in the course of the litigation (under the NSI Act) is less serious (in terms of conduct, but not necessarily consequence) than the deliberate communication of such information;

b. All of the other factors set out in a – f above in relation to the communication offences apply as well. This includes the fact the offences under s. 45A and s. 46FA of the NSI Act are arguably more serious than their ISA, ONI Act and ASIO Act equivalents as the prosecutor is required to prove under the NSI Act not just that there was a failure to comply with the Regulation but that the failure was likely to prejudice national security (this is not the case with the ISA/ONI Act/ASIO Act offences).

7. Similar offences under s. 122.1 and s. 122.2 of the Criminal Code also impose a 3 year penalty (or 5 years if aggravated under 122.3 – see below) for Commonwealth officers or someone engaged to perform work for a Commonwealth entity who:

- receive, obtain, collect, posses, record, copy, alter, conceal, publish or make inherently harmful information available (122.1(2));
- remove inherently harmful information from a proper place of custody or hold the information outside of a proper place of custody (122.1(3));
- fail to comply with a lawful direction resulting in a risk to the security of inherently harmful information (122.1(4));
- receive, obtain, collect, posses, record, copy, alter, conceal, publish or make *any information* (regardless of whether it is inherently harmful) available where doing so would cause harm, or likely to cause harm, to Australia's interests (122.2(2));
- remove *any* information (regardless of whether it is inherently harmful) from a proper place of custody or hold the information outside of a proper place of custody where doing so would cause harm, or likely to cause harm, to Australia's interests (122.2(3));
- fail to comply with a lawful direction regarding the retention, disposal or use of any information (regardless of whether it is inherently harmful) where doing so would cause harm, or likely to cause harm, to Australia's interests (122.2(4)).

## Aggravated Offences Under 122.3 of the Criminal Code

8. It is likely that some, or all, of the aggravating circumstances set out in s. 122.3 of the Criminal Code could apply to unlawful disclosures in contravention of the NSI Act. For example, NSI Act proceedings often include code word material and large numbers of documents with a security classification. Some of the people entrusted to protect national security information in legal proceedings will hold

security clearances (in fact Part 4 of the NSI Act contemplates that they may be provided with one for the purpose of the proceedings).

9. There are also other aggravating factors unique to the NSI Act offences which may not apply to the offences under the Criminal Code including, for example, the inherent vulnerability of large volumes of national security information in legal proceedings and the greater risk of it being exposed to hostile foreign intelligence services which makes deliberate non-compliance with the NSI Act more egregious than the conduct prohibited under s. 122.1, s. 122.2 and s. 122.3 of the Criminal Code.

## Why those entrusted with national security information in legal proceedings should be held to the same standards as those working with intelligence agencies or engaged to perform work for the Commonwealth, rather than members of the general public.

10. There are a small number of offence provisions in the Criminal Code which impose lesser penalties on those who are not Commonwealth officers and have not been engaged to perform work on behalf of a Commonwealth:

    - Section 122.4A imposes only a 5 year penalty for communicating secret or top secret information, or information that might damage the security or defence of Australia or harm or prejudice the health or safety of the Australian public.
    - Section 122.4A(2) imposes only a 2 year penalty for receiving, obtaining, collecting, possessing, recording, copying, altering, concealing, publishing or making available information if it has a secret or top secret classification, or doing so would damage the security or defence of Australia or harm or prejudice the health or safety of the Australian public.

11. The rationale for imposing lesser penalties on members of the public who disclose or mishandle national security information is that, unlike those working with intelligence agencies or the Commonwealth Government, they are not in a position of trust, they are unlikely to have access to significant volumes of classified information and they may be unaware of the sensitivity of the information or what is required to protect it. That rationale does not apply to people who commit offences under the NSI Act.

12. In explaining the higher penalties for those working in and with intelligence agencies (under the ISA and ASIO Act) the Explanatory Memorandum to the *National Security Legislation Amendment Act (No. 1) 2014* noted:

> 135. … Members of intelligence agencies are in a unique position of trust and power, and receive, often highly classified, information for the purpose of performing official duties and are aware of the procedures of handling such information and the consequences of disclosing that

> information. Given this, there is a strong and legitimate expectation that those persons will handle that information lawfully – that is, in strict accordance with their authority – at all times.

13. Those expectations are equally applicable to those entrusted to protect information under the NSI Act.

14. National security information is vulnerable in legal proceedings and is at far greater risk in that less secure environment than it is inside an intelligence agency or Secure Compartmented Information Facility (SCIF). We know that hostile foreign intelligence services seek to collect intelligence by targeting legal proceedings. Foreign intelligence services will often know, from media surrounding a trial, what type of national security information might be disclosed in the proceedings and who they should target. Court documents identify the judge and the parties' legal representatives, most of whom have public profiles and can be seen walking in and out of court with their clients. Foreign intelligence services are likely to expect that those involved in the proceedings, unlike members of the general public, will have access to large volumes of classified information and see them as a softer target.

15. Unlike members of the public, those involved in national security litigation are also in a unique position and do have a duty to protect the information they are entrusted with: they not only store and handle but *create* large volumes of classified information during proceedings, they are conscious of the sensitivities of the information and why it needs to be protected and they are given clear guidance (and provided with appropriate facilities and equipment) to ensure that it is stored and handled appropriately. Given this, there is also an appropriate expectation that they will handle the information lawfully and strictly in accordance with the NSI Act and Regulation.

16. The NSI Act will only work if all of those who are entrusted with national security information in legal proceedings (parties, their legal representatives, court staff, transcribers etc) take their obligations seriously and strictly comply with the requirements of the Act.