Australian Government

Attorney-General's Department

# *Submission to the Senate Legal and Constitutional Affairs Committee*

# *Intelligence Services Legislation Amendment Bill 2011*

The *Intelligence Services Legislation Amendment Bill 2011* (the Bill) was introduced into the Parliament on 23 March 2011.

This Bill makes amendments to the *Australian Security Intelligence Organisation Act 1979* (ASIO Act), the *Intelligence Services Act 2001* (IS Act) and the *Criminal Code Act 1995* (Criminal Code). The amendments have been identified through a targeted review and practical experience with the legislation relating to security and intelligence agencies. The amendments are aimed at improving the operation of some provisions of those Acts and addressing some key areas that have been identified as important from a practical and operational perspective. Legislation relating to national security agencies remains under constant review to address the challenges of the contemporary environment and ensure that the legislation continues to be appropriate for the dynamic national security environment.

**Foreign intelligence collection under the ASIO Act** [Items 3 and 5 – 15]

The Bill will amend the ASIO Act to align the definition of 'foreign intelligence' and the collection of foreign intelligence under the ASIO Act with the IS Act and *Telecommunications (Interception and Access) Act 1979* (TIA Act). This will ensure that the collection of foreign intelligence under the ASIO Act encompasses the same range of intelligence about state and non-state sponsored threats as covered by the term 'foreign intelligence' in those other Acts. Similar amendments to the TIA Act were made in the *Anti-People Smuggling and Other Measures Act 2010*. This will enhance interoperability and intelligence sharing between agencies, as 'foreign intelligence' will have a consistent meaning among the Australian Intelligence Community (AIC) agencies, which will enable more efficient processes and arrangements for collecting and communicating foreign intelligence.

ASIO's foreign intelligence collection function complements the functions of the foreign intelligence agencies. When the foreign intelligence function was initially conferred on ASIO, the key national security concern at the time was state sponsored threats. The definition of foreign intelligence in the ASIO Act reflected this, by defining foreign intelligence as 'intelligence relating to the capabilities, intentions or activities of a foreign power'.[1] Foreign power is defined as 'a foreign government; an entity that is directed or controlled by a foreign government or governments; or a foreign political organisation'[2].

[1] *Australian Security Intelligence Organisation Act 1979*, section 3.

[2] Ibid.

When the *Intelligence Services Act 2001* was drafted, the concept of foreign intelligence reflected in the functions of those intelligence agencies was intelligence 'about the capabilities, intentions or activities of people or organisations outside Australia', in so far as this relates to 'Australia's national security, Australia's foreign relations or Australia's national economic well-being'.[3] This concept of foreign intelligence reflects that modern national security threats come from both state and non-state sponsored threats. For example, terrorism, transnational crime, weapons proliferation and people smuggling are increasingly not sponsored by states, but rather by individuals or non-state sponsored organisations. As ASIO's foreign intelligence collection function complements the foreign intelligence collection function of the other intelligence agencies, it is desirable that ASIO be able to collect intelligence about the same spectrum of threats as those agencies. With the current differences between the ASIO Act and the IS Act, there is some potential for gaps in intelligence coverage as the ASIO Act definition of foreign intelligence is currently limited to intelligence about foreign powers.

In addition to amending the definition of foreign intelligence to provide consistency, it is also necessary to amend the provisions relating to foreign intelligence collection warrants and authorisations to align the collection of foreign intelligence under the ASIO Act and the IS Act. As noted above, the IS Act limits the concept of foreign intelligence by requiring that the agencies' functions 'are only to be performed in the interests of Australia's national security, Australia's foreign relations or Australia's national economic well-being'.[4] The current provisions in the ASIO Act enable the Attorney-General to issue a warrant or authorisation for ASIO to collect foreign intelligence if satisfied, on the basis of advice from the relevant Minister, that the intelligence is important in relation to the defence of the Commonwealth or the conduct of the Commonwealth's international affairs.[5] The proposed amendments will provide consistency with the IS Act by requiring the Attorney-General to be satisfied, on the basis of advice from the Defence Minister or Foreign Affairs Minister, that the collection of intelligence is in the interests of Australia's national security, Australia's foreign relations or Australia's national economic well-being. The effect of these amendments is that the collection of foreign intelligence under the ASIO Act will be consistent with the collection of foreign intelligence under the IS Act. ASIO's foreign intelligence collection function will therefore provide a consistent complementary role to the other agencies where it is necessary to collect foreign intelligence within Australia.

We note that the Law Council of Australia has raised concerns about the breadth of the amendment. Given that the objective is to ensure that ASIO's foreign intelligence function effectively complements the functions of the other foreign intelligence agencies, the relevant provision needs to reflect the same intelligence and the same purposes for which that intelligence may be obtained under the Intelligence Services Act. If not aligned, there are some potential gaps in Australia's intelligence coverage.

ASIO is only able to collect foreign intelligence at the request of the Minister for Foreign Affairs or the Minister for Defence, who are responsible for the foreign intelligence agencies. Additionally, the Attorney-General has to decide whether to issue a warrant or authorisation

---

[3] *See, Intelligence Services Act 2001,* section 11.

[4] Ibid.

[5] *Australian Security Intelligence Organisation Act 1979*, paragraphs 27A(1)(b) and s27B(b).

(based on advice from the relevant Minister), if satisfied that the collection of foreign intelligence in a particular matter is in the interests of Australia's national security, foreign relations or national economic well-being. ASIO's core focus is, and will continue to be, on security intelligence, such as counter-terrorism and counter-espionage. It is not expected that this amendment will result in significantly more foreign intelligence collection warrants or authorisations being issued under the ASIO Act.

**ASIO computer access warrants** [Item 4]

The Bill will also amend the ASIO Act to clarify that the intention was to authorise access to data held in the target computer at any time while the warrant is in force. This makes clear that the provision is intended to authorise access to data that is held in the target computer during the life of the warrant, and is not limited to data held at a particular point in time (such as when the warrant is first executed). This amendment is not intended to change the law, but rather to clarify the intent of the provision and ensure consistent language is used throughout the provision.

Currently, the computer access warrant provision uses different language in different subsections in relation to the same concept. Subsection 25A(2) refers to 'data *held* in a particular target computer', whereas paragraph 25A(4)(a) refers to 'data... *stored* in the target computer'. The proposed amendments will provide consistent language in the provision. The term data 'held' in the target computer is preferred as the more technologically neutral term. It would clearly encompass data that is stored on a more permanent basis, such as in a hard drive, as well as data that may be held in the computer on a temporary basis or from time to time, as is the intention of the provision. The amendment further clarifies this intent by providing that the Attorney-General may issue a computer access warrant 'for the purpose of obtaining access to data that is relevant to the security matters and is held in the target computer *at any time while the warrant is in force*'.

These amendments will not impact on the strong existing safeguards that ensure computer access warrants are only authorised in appropriate circumstances. A computer access warrant can only be issued by the Attorney-General in the prescribed circumstances set out in the provision – that is, the Attorney-General must be satisfied that there are reasonable grounds for believing that access by ASIO to data held in a particular computer will substantially assist the collection of intelligence... in respect of a matter that is important in relation to security[6]. Additionally, the Attorney-General's Guidelines, issued under section 8A of the ASIO Act, require that 'any means used for obtaining information must be proportionate to the gravity of the threat posed and the probabilities of its occurrence', and 'using as little intrusion into individual privacy as is possible'.[7] When a warrant is issued, the Director-General is required to report to the Attorney-General on the extent to which the warrant assisted ASIO in carrying out its functions.[8] ASIO is also subject to the oversight of the Inspector-General of Intelligence and Security, which is an independent statutory office

[6] Ibid, subsection 25A(2).

[7] *Attorney-General's Guidelines in relation to the performance by ASIO of its function of obtaining, correlating, evaluating and communicating intelligence relevant to security*, clause 10.4.

[8] *Australian Security Intelligence Organisation Act 1979*, section 34.

holder with responsibility for monitoring the legality and propriety of the activities of Australia's intelligence agencies and reporting to Ministers.

**ASIO information sharing of employment related information** [Items 16 – 18]

Part IV of the ASIO Act deals with the communication of information by ASIO to other Commonwealth agencies in the form of security assessments. The Bill will amend section 36 of the ASIO Act to exclude from the security assessment provisions in Part IV of the ASIO Act the communication by ASIO of information relating to the engagement, or proposed engagement, of a person by ASIO or by another intelligence or security agency within the AIC.

The amendment will allow ASIO to share more efficiently, information about employment decisions with other members of the Australian Intelligence Community (AIC). This might include information in response to inquiries about a person's employment or proposed employment with ASIO or another AIC agency, information about security clearances and other related information. Other AIC agencies are already able to share this information and are not subject to the same administrative requirements that apply to ASIO (which includes notification and review rights).

Within the AIC, employment decisions are undertaken by each individual AIC agency. Agencies will each have their own recruitment processes, but in general, applicants may be required to demonstrate suitable skills and competencies, as well as undergo security clearances. It is important to understand that a 'security clearance' is not necessarily the same as a 'security assessment' under the ASIO Act. A security clearance is a decision to grant a person access to information at a particular level (such as Top Secret). Within the AIC, security clearances are usually undertaken by the Defence Security Authority. A security assessment, on the other hand, is a statement in writing by ASIO to a Commonwealth agency, expressing any recommendation, opinion or advice on the question of whether it would be consistent with the requirements of security for prescribed administrative action to be taken.[9] Prescribed administrative action is defined broadly,[10] and would cover, among other things, a decision about employment within the AIC.

To explain the reason for the proposed amendment, it is perhaps useful to provide an example. Person A applies for a job with another AIC agency and their application is rejected due to security concerns about that person. AIC agencies do not provide feedback to unsuccessful applicants, so the person is not necessarily aware that this is the reason they were unsuccessful. Person A then applies for a job at ASIO. ASIO makes inquiries with other agencies, and the other AIC agency advises of the information that it obtained raising security concerns about the person. There is no requirement for ASIO or the other agency to provide the individual with feedback on their application or details of the information provided by the other AIC agency. However, if the situation is reversed, and Person A applies for a job with ASIO and then applies for a job with another AIC agency, if that AIC agency makes inquiries with ASIO, ASIO may only share that information in the form of a security assessment, and must therefore comply with the requirements of Part IV of the ASIO Act, which include providing notification and the availability of merits review. This is

[9] Ibid, section 35.

[10] Ibid.

a significant administrative burden that only applies to ASIO, and can impede information sharing on an issue as crucial as ensuring that people of security concern are not recruited into the AIC. The odd result of the above example is that the person could potentially seek merits review of the 'security assessment' that ASIO provides to the other AIC agency, but would have no similar appeal rights in relation to the actual decision of the other AIC agency about their employment.

This amendment will put ASIO on the same footing as other AIC agencies when it comes to sharing information relating to employment within the AIC. This is a very limited category of information, and the amendment will only impact on a small group of persons. Employment decisions within the AIC need to be made carefully, and necessarily the processes take quite some time compared to other Government employment processes in order to ensure suitability of applicants and minimise risk of compromising national security. It is therefore important that there are not unnecessary requirements and barriers that may inhibit information sharing or create inefficiencies in the AIC recruitment processes.

**Amendment to DIGO functions** [Item 21]

The Bill will amend the IS Act to provide the Defence Imagery and Geospatial Organisation (DIGO) with a function to specifically allow DIGO to provide assistance to the Australian Defence Force (ADF) in support of military operations and to cooperate with the ADF on intelligence matters. This is not an extension of the functions of DIGO but a clarification of them and is consistent with the similar function of the Defence Signals Directorate.

DIGO's functions are set out in section 6B of the IS Act. DIGO was added to the IS Act in 2005, following a recommendation of the *Report of the Inquiry into Australian Intelligence Agencies* (2004) conducted by Mr Philip Flood AO. Like DSD, DIGO is a part of the Defence Department, and it is only relatively recently that these agencies were established under legislation as separate agencies within Defence, with their own specific legislative mandate (DSD in 2001, and DIGO in 2005). As these two agencies are part of the Defence Department, it is inherent that a key part of their roles involves support to the ADF, and this is reflected in their functions. However, while DSD has a specific function to provide assistance to the ADF in support of military operations and to cooperate with the ADF on intelligence matters,[11] no mirror provision was included for DIGO when it was added to the IS Act. DIGO's ability to provide assistance and cooperate with the ADF comes under a number of separate functions. The advantage of having a specific provision to provide assistance and cooperate with the ADF on intelligence matters, rather than relying on the various individual functions, is that it makes reporting, compliance and related administrative processes much more efficient and would prevent any future gaps in DIGO's functions when assisting the ADF.

A discrete enabling function has the potential to further enhance operational cooperation between DIGO and elements of the ADF, particularly in support of the ADF's own intelligence collection activities. It would ensure that DIGO is able to mobilise and provide operational support and resources (including personnel, software and hardware) to ADF geospatial units, as required. Furthermore, it will facilitate DIGO's leadership and support

[11] *Intelligence Services Act 2001,* paragraph 7(d).

role to ADF units through the provision of expert technical assistance, raw data, and specialist equipment and compliance oversight.

DIGO also plays a significant role in the establishment and maintenance of technical geospatial standards within the Defence organisation. In discharging this responsibility, DIGO's activities include establishing priorities to ensure geospatial information interoperability across the ADF; evaluating geospatial information efforts during experiments, exercises and operations; and assisting with science and technology research and development priorities and programs. These tasks require DIGO to work closely with the ADF. A discrete function would clarify that the performance by DIGO of these activities is within the remit of DIGO's legislated functions under the IS Act.

**New ministerial authorisation ground** [Items 23 – 24]

The Bill will also provide a new ground for obtaining a Ministerial Authorisation for the purpose of producing intelligence on an Australian person under the IS Act. The requirement to obtain a Ministerial Authorisation before the foreign intelligence agencies can produce intelligence on Australian persons is an accountability mechanism to ensure that any intrusion on the privacy of Australians is limited to specified purposes and is approved by a Minister. Currently the relevant Minister can give an authorisation if satisfied that an Australian person is, or is likely to be, involved in one or more of the following activities:

- activities that present a significant risk to a person's safety;
- acting for, or on behalf of, a foreign power;
- activities that are, or are likely to be, a threat to security;
- activities related to the proliferation of weapons of mass destruction or movement of certain prohibited goods; and
- committing certain serious crimes.[12]

The new ground will apply where the Minister is satisfied that an Australian person is involved in, or likely to be involved in, activities related to a contravention of a UN sanction enforcement law.

UN sanction enforcement laws are laws specified by the Minister for Foreign Affairs under the *Charter of the United Nations Act 1945* because those laws give effect to Australia's international obligations under sanctions imposed by the United Nations Security Council (UNSC). The laws prohibit the unauthorised trade in specific goods and services that the UNSC has determined are contributing to the threat to or breach of international peace and security. The laws also prohibit making assets available to persons and entities designated by the UNSC for their contribution to these threats, and require their assets in Australia to be frozen.

UNSC sanctions, and Australian laws to give effect to those sanctions, are serious matters that relate to situations representing a threat to, or breach of, international peace and security. These situations include armed conflicts, terrorism and the proliferation of weapons of mass destruction. The measures required by UNSC sanctions, and Australia's UN sanction enforcement laws, ensure that the States, entities or individuals targeted by the sanctions

[12] Ibid, subsection 9(1A).

measures are denied access to the financial and material resources that fuel conflicts, or facilitate the commission of terrorist acts, or contribute to proliferation of weapons of mass destruction.

There is an increasing focus and requirement for intelligence on goods, services and other assets and financial resources being supplied to, or procured from, states, entities and individuals subject to UNSC sanctions. Some of the existing grounds for Ministerial Authorisations would cover some, but not all, such activities. The proposed amendment will avoid any gaps and will provide transparency as to the grounds for granting Ministerial Authorisations by having a specific ground relating to the contravention of UN sanction enforcement laws. This amendment will also ensure that the Government's intelligence requirements concerning breaches of UN sanctions are met.

**Clarification of immunity provisions in the IS Act and Criminal Code** [Items 19 and 26]

The Bill will amend the IS Act to clarify that the immunity provision in section 14 is intended to have effect unless another law of the Commonwealth, a State or Territory expressly overrides it. This provision provides immunity from civil and criminal activities for a limited range of circumstances directly related to the proper performance by the agencies of their functions. This limited immunity is necessary as certain Australian laws, including State and Territory laws, could impose liability on the agencies. The proposed amendment will not prevent other laws from limiting this immunity. However, the amendment will ensure that any such limitation cannot be done inadvertently, and will require express consideration to be given to whether section 14 should be overridden.

The Revised Explanatory Memorandum for the Intelligence Services Bill 2001 indicates that it was the intention when the provision was passed by Parliament in 2001 that section 14 was to provide immunity from civil and criminal liability for activities, carried out by the agencies in the proper performance of their functions, which might otherwise be prohibited by the unintended consequences of certain Australian laws. Section 14 is an important provision to provide protection for activities done in the proper performance of the functions of the agencies. It does not provide blanket immunity from Australian laws for all acts of the agencies, and reliance on the provision by the agencies is further regulated under Ministerial directions. If another provision needs to override section 14, then the other provision should clearly indicate that this is the case.

As currently drafted, the provisions are vulnerable to a law that is later-in-time inadvertently overriding them. This could occur particularly where an Australian law has extra-territorial effect. Parliament may choose to override this immunity in appropriate circumstances, but this amendment will ensure that there would need to be a conscious decision to do so and it would need to be made express on the face of the legislation.

A similar amendment will also be made to the immunity provision for the computer offences in Part 10.7 of the Criminal Code to clarify that the provision is intended to have effect unless another law of the Commonwealth, a State or Territory expressly overrides it. This provision mirrors the immunity provision in section 14 of the Intelligence Services Act, but specifically relates to computer offences, so it is desirable for these two provisions to maintain consistency.

The Revised Explanatory Memorandum for the Cybercrime Bill 2001 indicates that it was the intent when the provision was passed by Parliament in 2001, to provide immunity even where activities may otherwise be prohibited by Australian law. Amending section 476.5 would ensure that the original intent is preserved and cannot be inadvertently overridden. Section 476.5 is an important provision to provide protection for activities done in the proper performance of the functions of the agencies. If another provision needs to override section 476.5, then the other provision should clearly indicate that this is the case.

**Legislative instruments amendments** [Items 20, 22, 27 and 28]

The Bill will also amend the IS Act to place existing exemptions from the *Legislative Instruments Act 2004* in the IS Act rather than in the *Legislative Instruments Regulations 2004*. This is consistent with the Government's commitment to clearer laws, as the status of certain instruments under the IS Act will be clear on the face of that Act. This approach was supported by the *Report of the Review of the Legislative Instruments Act* (2008)[13].

The existing exemptions, currently set out in the Legislative Instruments Regulations, apply to instruments made under paragraph 6(1)(e) (Ministerial directions in relation to ASIS activities), section 8 (Ministerial directions to agencies), section 15 (Privacy Rules), and clause 1 of Schedule 2 (guidelines for the use of weapons and self defence techniques). These amendments will not change the existing law.

[13] *Report of the Review of the Legislative Instruments Act 2003* (2008) by the Legislative Instruments Act Review Committee.