TELECOMMUNICATIONS INTERCEPTION AND INTELLIGENCE SERVICES LEGISLATION AMENDMENT BILL 2010

SENATE LEGAL AND CONSTITUTIONAL AFFAIRS LEGISLATION COMMITTEE

Responses to Questions on Notice and Supplementary Information

Attorney-General's Department

Senator Barnett asked a question at the hearing on 11 November 2010 about how long it would take to consult with stakeholders and review the Attorney-General's Guidelines for ASIO and the Privacy Rules for ASIS, DSD and DIGO.

The answer to the honourable Senator's question is as follows:

This question arose in the context of a suggestion put forward by the Office of the Australian Information Commissioner that consideration be given to establishing a privacy framework or memorandum of understanding (MOU) in relation to the use and disclosure of information between the security, intelligence and law enforcement agencies that will be covered by measures in the Bill.

As indicated at the hearing, the security and intelligence agencies are covered by existing Attorney-General's Guidelines[1] and Privacy Rules[2], which apply privacy

[1] Section 8A of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) provides that the Minister may give the Director-General guidelines to be observed in the performance by ASIO of its functions. Those guidelines are to be tabled in Parliament. The current Guidelines include privacy requirements and considerations (for example, see clauses 10 and 13).

[2] Section 15 of the *Intelligence Services Act 2001* provides that the Minister responsible for ASIS, DIGO and DSD must make written rules regulating the communication and retention by the relevant agency, of intelligence information concerning Australian persons. The agencies must not communicate intelligence information concerning Australians, except in accordance with the Privacy Rules. The Intelligence Services Act also specifies certain consultation requirements.

principles in so far as is consistent with the functions and responsibilities of those agencies. Both the Attorney-General's Guidelines and the Privacy Rules are made under statutory provisions, and the agencies are legally bound to comply with them. Compliance with the Attorney-General's Guidelines and Privacy Rules is subject to independent oversight by the Inspector-General of Intelligence and Security, who reports annually to Parliament.

Active consideration has been given to privacy issues in the development of this Bill, including whether the existing Attorney-General's Guidelines and Privacy Rules remain appropriate. In light of the existing privacy regimes, the Attorney-General's Department is of the view that additional privacy frameworks or MOUs do not appear to be necessary. The existing privacy regimes will continue to be reviewed and revised as appropriate to ensure they continue to balance operational considerations with appropriate privacy protections.

It may assist the Committee to note that once any internal review is undertaken by relevant agencies and Departments, there are certain requirements under the legislation that must be complied with for new or revised Attorney-General's Guidelines or Privacy Rules. This includes requirements to consult with certain persons[3], provide copies to the Inspector-General of Intelligence and Security and the Leader of the Opposition,[4] and arrangements for briefing of the Parliamentary Joint Committee on Intelligence and Security.[5] It is also noted that the decision to issue new or revised Attorney-General's Guidelines or Privacy Rules is a decision for the relevant responsible Minister.

It is difficult to provide a definitive answer to the Committee as to how long it would take to consult with relevant stakeholders and review the Attorney-General's Guidelines and the Privacy Rules, as this may depend upon the nature and scale of any such review, and may be affected by other related developments. As was indicated at the hearing, there are some broader privacy related reforms currently on

[3] *Intelligence Services Act 2001*, s 15(3).

[4] *Australian Security Intelligence Organisation Act 1979*, s 8(5) and (6).

[5] Ibid, s 8A(6); *Intelligence Services Act 2001*, s15(6).

foot. On 24 June 2010, the then Cabinet Secretary, Senator the Hon Joe Ludwig, released an Exposure Draft of proposed changes to the development of a single set of Australian Privacy Principles. This forms part of the Government's First Stage Response to the Australian Law Reform Commission's report, *For Your Information: Australian Privacy Law and Practice* (2008).[6] The Exposure Draft is currently being considered by the Senate Finance and Public Administration Committee, which is due to report by 1 July 2011. Once that broader work has been completed, it may then be an appropriate time to re-examine the Attorney-General's Guidelines and the Privacy Rules. This is consistent with existing policy of aligning the Attorney-General's Guidelines and the Privacy Rules with the privacy principles under the *Privacy Act 1988* in so far as is consistent with the functions of those agencies.

Senator Barnett asked a question at the hearing on 11 November 2010 about further particulars regarding the imperative in terms of timing for the Bill.

The answer to the honourable Senator's question is as follows:

The Bill contains important measures to ensure Australia's security and intelligence agencies continue to be well placed to respond to national security threats. As recognised in the 2008 National Security Statement, modern national security challenges are increasingly complex and inter-connected. A well-integrated intelligence community is essential to Australia's ability to respond to modern national security challenges. There are some limitations on the extent of cooperation and intelligence sharing between security and intelligence agencies within the existing legislative framework.

As indicated at the hearing, in line with the National Security Statement, the Smith Review of Homeland and Border Security and more recently the Counter-Terrorism White Paper, there has been ongoing active consideration directed towards ensuring that there are not unnecessary barriers to cooperation and intelligence sharing among

[6] Further information about privacy reforms is available on the Department of the Prime Minister and Cabinet's website at: http://www.dpmc.gov.au/privacy/reforms.cfm.

the intelligence community. Recent events, such as the failed bombing of flight NW253 on 25 December 2009 in the United States, are a timely reminder of the need to remain vigilant to national security threats. To ensure that agencies are in the best possible position to identify and respond to such threats, there needs to be appropriate and efficient mechanisms for cooperation and intelligence sharing between relevant intelligence agencies. The amendments in Schedule 6 of the Bill go towards facilitating closer cooperation and intelligence sharing among Australia's key intelligence agencies, and it is therefore desirable for these measures to be considered in a timely fashion.

A further timing imperative relates to the amendments that facilitate ASIO providing technical assistance and intercepting on behalf of other agencies. As the complexity of the available technology increases at a rapid rate there is a clear need for government agencies to harness and utilise resources in the most effective manner. ASIO has a lead agency role to provide technical advice relating to telecommunications interception to all interception agencies. The National Interception Technical Assistance Centre (NITAC) pilot program commenced on 1 July 2010 and is intended to operate for two years. With assistance from the AFP, ASIO will provide coordinated technical assistance to other Australian interception agencies by providing a central point of reference from which agencies can receive technical assistance to help keep pace with technical change.

While some of the measures intended by the NITAC program are able to operate under current legislation, the proposed amendments in the Bill will ensure the pilot is able to fully function in the remainder of the two year period. In developing the amendments all safeguards that maintain the integrity of the interception regime have been upheld.

Senator Barnett asked a question at the hearing on 11 November 2010 about whether the provisions in Schedule 2 of the Bill in relation to the requirement for industry to advise the Communications Access Coordinator of certain matters could be better expressed.

The answer to the honourable senator's question is as follows:

The Department does not consider that changes are needed to Schedule 2 of the Telecommunications Interception and Intelligence Services Legislation Amendment Bill.

Schedule 2 reintroduces an obligation that was removed from the *Telecommunications Act 1997* in 2007 when the Interception Capability Plan (ICP) scheme was transferred to the *Telecommunications (Interception and Access Act) 1979* (TIA Act). An ICP, in Part 5-4 of the TIA Act, outlines how the industry participant will meet their interception obligations. However, the Department has found that the ICP process has not provided a mechanism that facilitates notice sufficiently early in the development of a change to allow for effective consultation.

The proposed amendment will require industry to inform the Communications Access Coordinator (CAC) in a timely manner of changes to telecommunications services, networks, systems or devices which would adversely affect their ability to meet their legal obligation to assist national security and law enforcement agencies. Allowing Government to work with industry during the development stage may reduce industry's regulatory compliance costs by avoiding the need for costly unplanned re-working of non-compliant services.

Notification can be as simple as forwarding a letter to the CAC that outlines the intended changes and how legal obligations will continue to be met.

Carriers and nominated carrier service providers (C/NCSPs) are part of the Australian telecommunications industry, and are well aware of their legal obligations with respect to telecommunications interception. Nominated carriage services providers are carriage service providers which are declared under subsection 197 of the TIA Act

because of their level of involvement in the industry and their particular need for effective interception capability.

The majority of notified network changes will have no impact on legal obligations and changes that do impact on legal obligations necessarily require C/NCSP consideration about whether they can continue to meet their regulatory obligations. The notification requirement uses the same language and applies in the same circumstances as current section 201(2) of the TIA Act, which deals with the consequences of changed business plans. Therefore, the industry is already experienced at identifying these types of changes. The CAC typically receives fewer than 5 updated ICPs per annum pursuant to section 201. However, this does not reflect the full number of changes to services or networks which affect legal obligations and therefore warrant notification.

The Department notes that industry participants have expressed the view that amendments to the ICP arrangements would be a simpler way to achieve the outcomes that Schedule 2 pursues.

An ICP must set out the matters provided for in section 195(2) of the TIA Act, including a statement of interception policies, strategies for legal compliance and a list of employees with responsibility for interception. ICPs must be approved by the carrier's CEO or an officer approved by a CEO. As such, ICPs are an extensive document which requires considerable resources to prepare and submit. Section 201 requires ICPs to be updated in the same circumstances as those in which Schedule 2 applies. Regrettably, section 201 has not facilitated effective government involvement prior to relevant changes being implemented. For example, there are several instances where carriers or their third party outsource providers have committed to changes without timely consultation with agencies. This has resulted in avoidable and costly re-working. These new provisions will empower those people within the carriers who manage agency related matters to manage such situations more effectively and efficiently.

The purpose of the obligation in Schedule 2 is to provide a mechanism to inform the CAC before the implementation of relevant changes, rather than afterwards. The

Department considers that supplementing the ICP process with the Schedule 2 obligation places less of a burden on industry than an amendment to the ICP process.

The 30 day period proposed in subsection 202B(6) places a strict timeline, as well as the onus of action, on Government not on industry. It should be noted that the CAC does not have a veto power over proposed changes.

The purpose of the 30 day period is to require Government to engage with industry in a timely manner to discuss possible impacts on industry's ability to meet their regulatory obligations. Industry will continue to be bound by the obligations in the TIA Act and the *Telecommunications Act 1997* to have interception capability.

As a general rule, notification as early as possible will facilitate the CAC and agencies providing timely advice to C/NCSPs without detriment to the roll out of services.

The Chair asked a question at the hearing on 11 November 2010 seeking the Department's response to the fourth recommendation by the Office of the Australian Information Commissioner in relation to clarifying the Explanatory Memorandum to provide guidance on when it may be impracticable to consent under the proposed amendments in Schedule 4 of the Bill.

The answer to the honourable senator's question is as follows:

Schedule 4 to the Bill removes ambiguity in the existing language in the TIA Act to clarify that an enforcement agency may obtain a stored communications warrant to access the stored communications of the victim of a serious contravention where the victim cannot be notified. A warrant may only be issued by an issuing authority who is a judge or nominated Administrative Appeals Tribunal member. The issuing authority will still be required to consider a wide variety of factors before issuing a warrant, including how the privacy of the person would be impacted by the issue of a warrant. Enforcement agencies who obtain a stored communications warrant will continue to be required to meet record keeping and public reporting obligations.

The Explanatory Memorandum states that the situations where the access to the stored communications of a victim of a serious contravention crime may occur are where the person is unable to consent or it is impracticable for them to consent. It was not thought necessary for the Explanatory Memorandum to be too prescriptive about those issues, as it is a question of fact to be determined in the circumstances of each case. The decision is a matter for the issuing authority, who should have sufficient flexibility to make a decision about the circumstances relating to victim notification in individual applications.

Section 116(2) sets out matters that must be considered by an issuing authority before issuing a stored communications warrant, which are not affected by the amendment. The issuing authority must have regard to all of the following matters:

- how much the privacy of the person would be likely to be interfered with,
- the gravity of the conduct constituting the serious contravention,
- how much the information would be likely to assist with the investigation of the serious contravention,
- the extent to which other methods of investigating that do not involve the use of a stored communications warrant have been used,
- how much the use of such methods would be likely to assist in connection with the investigation, and
- how much the use of such methods would be likely to prejudice the investigation by the agency because of delay or for any other reason.

In respect of issuing a stored communications warrant for a victim, the issuing authority must consider if the victim is able to be notified. The Explanatory Memorandum intends to provide guidance to the issuing authority by stating that a victim is unable to be notified if the victim is missing, deceased or incapacitated.

Supplementary information – Schedule 3 – Missing Persons

Submissions have raised concerns about the level of consideration given to the intrusion on privacy of personal information in developing the Bill. Privacy implications were actively considered during the policy development of the Bill, and we note that there are comprehensive privacy mechanisms and safeguards that apply to the activities of the agencies covered by the measures in this Bill.

To provide clarity about this issue, we thought it would be beneficial to highlight the privacy protections in Schedule 3.

Telecommunications data is information about a communication. It does not include the content of a communication. Currently historical telecommunications data (data that is in existence) can be accessed under the TIA Act by an enforcement agency for the enforcement of a criminal law, a law imposing a pecuniary penalty or the protection of the public revenue. Prospective telecommunications data (data that is not yet in existence) can be accessed by a defined criminal law enforcement agency for the investigation of a criminal offence punishable by imprisonment for at least three years. The access to data regimes includes safeguards such as an offence for inappropriate disclosure or use of the information and agencies have record-keeping and public reporting obligations.

The proposed amendments in Schedule 3 would allow a Police Force to access historical telecommunications data for the purposes of locating missing persons. The amendments uphold all safeguards that currently exist in the telecommunications data regime. The amendments include additional safeguards about the disclosure and use of information to ensure that Police only disclose or use information if it is for the benefit of a missing person. The extra controls recognise that this information is for public safety and not for criminal investigation purposes. The amendments will respect that not all missing persons want their location divulged and may not consent to the disclosure or use of information.

Additional safeguards premised around the notion of ‘consent’ ensure that disclosure of information prior to a missing person being located is only permitted for the

purpose of finding the person and not for informing family of 'signs of life'. Further, the safeguards ensure that a person who is privy to information may only disclose or use the information if:

- it is reasonably necessary for the purpose of finding the missing person, or
- information is disclosed to the notifying person and the missing person consented, or
- the missing person is unable to consent and disclosure is reasonably necessary to prevent a threat to the person's health, life or safety, or
- the person is deceased.

The unauthorised disclosure or use of accessed information will be subject to an offence punishable by two years imprisonment. These amendments will ensure the privacy of a missing person will be respected.

Supplementary information – Schedule 6 – Cooperation and Intelligence Sharing

Having read the Submissions provided to the Committee, we note that a number of Submissions raised concerns or asked questions about some of the amendments in Schedule 6. We thought that it may further assist the committee if we provided some additional information about the measures in Schedule 6.

The amendments to the *Australian Security Intelligence Organisation Act 1979* and the *Intelligence Services Act 2001* in Schedule 6 are intended to address three separate, though related, policy objectives. These are:

- enabling ASIO to cooperate and assist law enforcement agencies, primarily so as to facilitate technical assistance for interception, including through the National Interception Technical Assistance Centre (NITAC);
- enabling ASIO, ASIS, DSD and DIGO to cooperate more closely and assist one another to ensure a well-connected intelligence community;
- amending the ASIO Act communications provisions to provide ASIO with sufficient flexibility to communicate intelligence with the other intelligence

agencies (to complement the cooperation amendment above) and also to address limitations identified through practical experience with the legislation.

Cooperation and assistance to law enforcement agencies

Item 17 includes an amendment that will enable ASIO to cooperate and assist a law enforcement agency, which is an important provision to facilitate the operation of the NITAC. As indicated in our Submission to the Committee, law enforcement agencies face challenges from rapid technological changes that impact on their ability to gain lawful access to highly valuable evidence through telecommunications interception. The NITAC pilot program is of key importance in responding to the rapid technological change, by enabling interception agencies to harness resources and work cooperatively on technical matters. This may include general cooperation on technical matters to maintain an effective and efficient interception capability for all agencies, and may also extend to providing assistance to other agencies in the form of intercepting on their behalf. The technological challenges faced in this area are not matters that can be dealt with by simply providing more training or resources to law enforcement agencies.

While the key policy objective for this measure is to facilitate ASIO technical assistance to law enforcement agencies in relation to telecommunications interception, the amendment will enable other forms of assistance to be provided in appropriate circumstances, which would need to be agreed between agency heads. The type of other assistance that could be provided might include technical assistance on other matters and analytical assistance. Any such assistance would have to be considered within the context of ASIO's resources and other operational priorities. ASIO does not have powers of arrest, and gathering evidence for prosecution purposes is a matter for police. The delineation between law enforcement and security has been well maintained in the counter-terrorism area, as evidenced in the ASIO/AFP National Counter-Terrorism Protocol, which was established in accordance with the recommendations of the Street Review.[7] It is not expected that the new cooperation

[7] *A Review of Interoperability Between the AFP and its National Security Partners* (2008). Note that the National Counter-Terrorism Protocol is an operational level document and is therefore not publicly available.

provision risks blurring the distinction between security and law enforcement agencies.

Item 7 of Schedule 6 contains a definition of 'law enforcement agency'. As this definition ties in with the agencies that ASIO can assist for the purposes of the NITAC, the definition needed to cover bodies with the ability to intercept telecommunications being agencies with functions that relate to law enforcement, but which are not considered to be traditional police bodies. In particular, the definition needed to be sufficiently broad to cover police integrity and anti-corruption bodies such as the Australian Commission for Law Enforcement Integrity. There are many different definitions of law enforcement agency throughout different pieces of legislation, which vary depending upon the context of the particular Act, and other definitions were considered in drafting this Bill. The definition included in Item 7 was considered to be the most appropriate definition to cover those agencies that need to be covered for the purposes of the measures in this Bill.

Cooperation and assistance among the intelligence agencies

Items 17 and 27 of Schedule 6 make amendments to the ASIO Act and the Intelligence Services Act respectively, to provide a mechanism for closer cooperation and assistance between four of Australia's intelligence agencies – ASIO, ASIS, DSD and DIGO. This amendment is necessary to address some inherent limitations within the existing legislation, which can prevent cooperation on key national security priorities from occurring to their fullest extent. The limitations are elaborated upon further below.

ASIO has both intelligence collection and assessment functions, but ASIS, DSD and DIGO have functions relating to foreign intelligence production but not assessment. This can result in limitations on the cooperation or assistance which the latter agencies can provide to ASIO in relation to its security intelligence assessment functions. This has implications for multi-agency teams and taskforces that have assessment related roles.

Multi-agency teams and taskforces are designed to draw together a range of agencies to pool their diverse range of capabilities and resources to focus on key national security issues. Such teams have become an increasingly utilised mechanism for responding to whole-of-government national security priorities. While the agencies involved in such teams will have mutual interest in the subject matter of the multi-agency team, divergence in their legislative functions can create obstacles to full cooperation within the multi-agency team. For example, agencies under the Intelligence Services Act have functions that concern 'intelligence about the capabilities, intentions or activities of people or organisations outside Australia'[8] as relevant to Australia's national security, foreign relations or national economic wellbeing[9]. In comparison, ASIO's functions relate to security, which encompasses security threats to Australia and Australian interests (which is not limited by geographical boundaries). The divergence of functions can create difficulties for multi-agency teams if they seek to perform activities that have a broad focus on threats to national security both domestically and internationally.

As we have noted previously, the decision to cooperate under these provisions will be a matter for relevant agency heads, as it is a matter appropriate for them to consider in light of their operational priorities and resources. The Bill specifically requires that any such cooperation or assistance must comply with any relevant Ministerial directions that may be issued. This is consistent with the existing principle of Ministerial responsibility, and consistent with existing provisions in the ASIO Act and Intelligence Services Act that enable Ministers to provide guidelines or directions to their relevant agencies.[10] We also note that there are a range of strong accountability and oversight mechanisms already in place under existing legislation, which will apply to the cooperation and assistance arrangements. In particular, the Inspector-General of Intelligence and Security (IGIS) will continue to have oversight of the agencies' activities, and compliance with relevant laws and Ministerial guidelines and

[8] *Intelligence Services Act 2001,* ss 6, 6B, 7.

[9] Ibid, s 11(1).

[10] See, eg, *Australian Security Intelligence Organisation Act 1979*, ss 8, 8A; *Intelligence Services Act 2001*, s 8,

directions, consistent with its existing oversight role. As we noted at the hearing, the IGIS's role includes considering both the legality and the propriety of the activities of agencies, and therefore provides a strong mechanism for ensuring the new cooperation provisions are not being used for inappropriate purposes.

Intelligence sharing

Item 12 of Schedule 6 makes a number of amendments to the ASIO Act communications provisions to provide ASIO with the necessary flexibility to communicate intelligence with the other intelligence agencies and address some matters that have been identified through practical experience with the operation of the legislation.

The proposed new subsection 18(4A) will complement the cooperation provisions outlined above, by ensuring that ASIO has similar capacity to share intelligence with the other intelligence agencies. This will provide greater consistency with the intelligence sharing provisions under the Intelligence Services Act.[11] This forms a key part of ensuring that Australia's intelligence agencies are well-connected and efficiently able to share intelligence.

The other amendments to section 18 of the ASIO Act address a number of matters that have been identified through practical experience with the operation of the Act. This includes the provisions enabling information to be communicated if relevant to a serious crime or in the national interest. The amendments are intended to enhance the flexibility of existing provisions, and are not intended to result in a significant expansion of the information that may be communicated by ASIO. As Mr Fricker explained at the hearing, decisions to communicate information under these provisions are serious decisions, taken at senior levels of ASIO, and ASIO is not intending to have a 'spin-off line of business' in providing a trickle of information to various other agencies.[12] While the amendments provide greater flexibility as to the persons and agencies to whom ASIO may communicate information (which will

[11] See eg, *Intelligence Services Act 2001*, ss6(1)(b), 6B(d), 7(b).

[12] Proof Committee Hansard, Senate Legal and Constitutional Affairs Legislation Committee, 11 November 2010, p 25.

enable more efficient communication), it is not the expectation that this will significantly expand the circumstances under which ASIO would decide to communicate information under those provisions.

In addition to the relevant legal thresholds that must be met under section 18(3) for information to be communicated, there are also important requirements for the communication to be authorised in accordance with section 18(1) of the ASIO Act. Unauthorised communication of information by an ASIO officer constitutes an offence.[13] As noted elsewhere, ASIO must also comply with the Attorney-General's Guidelines. Further, the communication of information is a discretionary matter, and ASIO will also need to consider operational implications, such as the risk of direct or inadvertent compromise of sources, capabilities and operational methods.

The definition of 'serious crime' in Item 4 will replace the current reference to 'indictable offence' in subsection 18(3) of the ASIO Act. It has been defined as an offence punishable by a period exceeding 12 months, so as to provide consistency with other Commonwealth legislation, including the definition of 'indictable offence' in section 4G of the *Crimes Act 1914*.[14] While indictable offence has different meanings in some other jurisdictions[15], we consider it preferable to have consistency across Commonwealth legislation on this issue.

We note that some submissions have queried the meaning of national interest, which is used in existing subsection 18(3)(b) of the ASIO Act. That provision is being amended by Item 12, but no change to the term national interest itself is proposed. The term 'national interest' is used in other contexts in Commonwealth legislation where it is also not defined[16]. Courts, when considering decisions made on grounds of national interest in other contexts, have generally expressed views indicating that the primary determination of what is in the national interest is for the Minister.[17] In a

[13] *Australian Security Intelligence Organisation Act 1979*, s 18(2).

[14] See also, *Intelligence Services Act 2001*, s 3.

[15] See, eg, *Legislation Act 2001* (ACT), s 190.

[16] See eg, *Trade Practices Act 1974,* s *5(5).*

[17] See eg, *Wong v MIMIA*, 6 August 2002, BC 200224349 at [33].

democracy, it is appropriate for the Government of the day to set its priorities and determine what is in the national interest. The types of matters that might be encompassed by the term may include matters of importance to Australia's international relations or to sustaining the economy. In the national security context, national interest may be informed by the National Security Statement and the National Intelligence Priorities, which are set by the Government and reviewed on at least an annual basis.

We also note that Senator Barnett posed a question to the Law Council and to ASIO at the hearing as to whether the amendments in Schedule 6 would enable ASIO to communicate information it collects to ASIO's Minister under these provisions. We would like to clarify that the amendments in Item 12 do not provide ASIO with any new capacity to collect information – the amendments relate to the communication of information that is obtained incidentally in the course of ASIO's security functions. As Mr Fricker noted, ASIO is required to report to the Attorney-General in relation to the effectiveness of its warrants and keep the Attorney-General informed in relation to ASIO's priorities and activities. However, these are separate matters to the communications provisions in section 18. The provisions in section 18 could enable ASIO to communicate information relevant to a serious crime or in the national interest to the Attorney-General, or to another Minister, if that information related to a serious crime or was in the national interest and was relevant to the Minister's portfolio responsibilities as a particular Minister. It is important to note that this would not authorise the communication of information to a Minister for purposes of a political nature. Section 20 of the ASIO Act charges the Director-General of Security with special responsibility to:

> *take all reasonable steps to ensure that:*
>
> *(a) the work of the Organisation is limited to what is necessary for the purposes of the discharge of its functions; and*
>
> *(b) the Organisation is kept free from any influences or considerations not relevant to its functions and nothing is done that might lend colour to any suggestion that it is concerned to further or protect the interests of any particular section of the community, or with any matters other than the discharge of its functions.*

As stated earlier, all ASIO's activities, including its use and disclosure of information, are subject to the oversight of the IGIS, who actively considers not only issues of legality, but also matters of propriety.