Acting Independent National Security Legislation Monitor
Inquiry into section 35P of the ASIO Act
Attorney-General's Department response to request for information

Question 1: Role of the Department in the operation of Division 4 of Part III

(1) Does the Department have a role, or is it contemplated that the Department may have a role, in the operation of Division 4 of Part III of the ASIO Act? Please particularly address any role, or contemplated role, in relation to the following matters:

(a) providing third-party advice to the Attorney-General in the consideration of ASIO's applications for authorities to conduct special intelligence operations made under section 35B. (For example, under similar arrangements to the Department's assurance function in relation to warrant requests made under Division 2 of Part III);

Department's Response:

The Department will have a role in some aspects of the operation of Division 4 of Part III of the *Australian Security Intelligence Organisation Act 1979*.

(a) The Department has had for some time, and continues to have, a role in examining ASIO's applications to the Attorney-General for warrants under Division 2 of Part III of the ASIO Act, for the purpose of providing assurance that the applications comply with legislative requirements. The Department assesses the applications against the legislative requirements and liaises with ASIO on any concerns or suggestions before the applications are put to the Attorney-General.

It is not envisaged that the Department will have the same kind of role in relation to Special Intelligence Operations (SIO) applications because of the greater operational sensitivity and risks associated with SIO information and the need to very strictly confine and control the dissemination of that information. However, the Department will have a role in examining template documentation to ensure relevant legislative issues are address in SIO applications. The Department would also provide advice or assistance if the Attorney-General or ASIO wish to raise particular matters with the Department.

(b) providing advice or other assistance to the Attorney-General in considering reports made under section 35Q, or any oversight reports provided by the Inspector-General of Intelligence and Security (IGIS) under the *Inspector-General of Intelligence and Security Act 1986* about the legality and propriety of ASIO's activities under Division 4 of Part III;

Department's Response:

It is envisaged that the Department will play the same kind of role in relation to reports under the SIO regime as it does for other kinds of ASIO and IGIS reporting on the use of ASIO powers. The extent of any Departmental involvement will always depend on the particular issues covered by the reports.

The Department is not generally involved in the Director-General's reports to the Attorney-General on the use of warrant powers, but can provide assistance and advice to the Attorney-General if ASIO or the Attorney-General requests input from the Department.

In relation to oversight reports by the Inspector-General of Intelligence and Security (IGIS) under the *Inspector-General of Intelligence and Security Act 1986*, the usual practice (subject to any considerations concerning the particular subject matter, sensitivity and relevance of issues to the Department) is for the Attorney-General's Office to refer such reports to the Department for appropriate consideration, consultation and advice on any appropriate action. It is expected the Department will play a similar role in relation to IGIS reports on the legality and propriety of ASIO's activities under Division 4 of Part III of the ASIO Act.

(c) providing advice to the Attorney-General in considering any requests for his or her consent to a prospective prosecution under section 35P, pursuant to the Attorney-General's direction to the CDPP of 30 October 2014 under section 8 of the *Director of Public Prosecutions Act 1983*;

Department's Response:

The Department is not involved in operational matters such as decisions to investigate particular matters or the assessment of briefs of evidence, but does have a role in the seeking of the Attorney-General's consent where required to commence proceedings for certain offences. These include foreign incursion offences and genocide, crimes against humanity and war crimes in Divisions 119 and 268 of the *Criminal Code Act 1995*.

It is a matter for the Commonwealth Director of Public Prosecutions (CDPP) to determine, in accordance with the *Prosecution Policy of the Commonwealth*, whether to proceed with a prosecution. If that decision is made in relation to an alleged offence by a journalist against section 35P of the ASIO Act, the CDPP is required to seek the consent of the Attorney-General to commence proceedings. Consistent with the usual practice applying to other prosecutions requiring the Attorney-General's consent, the CDPP will liaise with, and provide relevant information to, the Department, who will consider the matter, brief the Attorney-General, and obtain a decision on the granting or otherwise of consent.

(d) any engagement with ASIO, the AFP or the CDPP in the course of the investigation or enforcement of offences against section 35P.

Department's Response:

While the Department is not involved in operational matters such as the investigation or enforcement of offences, the Department may be consulted by the AFP, ASIO or the CDPP during the course of such matters for advice on the legislation the Department administers, including the ASIO Act, the *Crimes Act 1914*, the Criminal Code and the *National Security Information (Criminal and Civil Proceedings) Act 2004*. In particular, the Department may be consulted on the application and operation of certain provisions in the legislation and the interaction between provisions.

Questions 2-5: Use or contemplated use of special intelligence operations

(2) To the Department's knowledge, have any applications under section 35B of the ASIO Act been made to the Attorney-General, seeking authority to conduct a special intelligence operation under section 35C? If yes, please provide details.

(3) In the event that the Department is aware of any special intelligence operations that have been authorised under section 35C and have commenced, is the Department aware of any reports being provided to the Attorney-General and the IGIS under section 35Q? If yes, please provide details, particularly whether the Department is aware of any reporting of the matters prescribed by subsection 35Q(2A).

(4) In the event that the Department is aware of any special intelligence operations that have been authorised under section 35C and have commenced, is the Department aware of whether any participants in such operations have, or are alleged to have, engaged in conduct of a kind described in paragraphs 35C(2)(d) and 35(2)(e) in the course of an operation? If yes, please provide details.

(5) In the event that the Department is aware of any special intelligence operations that have been authorised under section 35C and have commenced, is the Department aware of any contraventions or alleged contraventions of section 35P? If yes, please provide details.

Department's Response:

The Department will respond to these questions separately.

Questions 6-7: Experience with disclosure offences applying to Commonwealth controlled operations, assumed identities and witness protection schemes under the Crimes Act 1914.

(6) Further to the Department's evidence to the Parliamentary Joint Committee on Intelligence and Security inquiry into the (then) National Security Legislation Amendment Bill (No 1) 2014, is the Department aware, as at March 2015, of any referrals of matters for investigation, investigations undertaken, or referrals for prosecution relating to the disclosure offences identified in paragraphs (a)-(c) below?

If yes, please provide details, particularly as to whether any persons under investigation are journalists reporting on operational matters.

(a) Sections 15HK and 15HL (controlled operations).

(b) Section 15LC (assumed identities).

(c) Section 15MS (witness protection for law enforcement operatives).

Department's response:

The Department is not aware of any referrals of matters for investigation, investigations undertaken, or referrals for prosecution relating to sections 15HK, 15HL, 15LC, or 15MS of the Crimes Act. However, it may be that one or more of the subjects referred to above has been considered by the AFP and / or the CDPP and they will be able to provide information to the inquiry about those matters.

(7) Is the Department aware of any reports made to the Attorney-General and the Commonwealth Ombudsman in relation to controlled operations and assumed identities (or the IGIS in the case of assumed identities of ASIO officers) under the following provisions of the Crimes Act, which

have identified instances of wrongdoing or conduct that exceeds the limits of the relevant authority?

(a) Sections 15HM, 15HN and 15HO (reports on controlled operations), particularly with respect to the matters prescribed in paragraphs 15(2)(r) and (s), concerning loss of or serious property damage or personal injuries occurring in the course of or as a direct result of the operations in the reporting period.

(b) Sections 15LD and 15LE (reports on the use of assumed identities), particularly with respect to the matters prescribed in paragraphs 15LD(1)(f) and 15LE(f) concerning the identification of fraud or unlawful activity relating to the use of assumed identities in the course of mandatory audits completed under section 15LG.

Department's response

The Department is not aware of any reports made to the Attorney-General or the Commonwealth Ombudsman in relation to assumed identities (or the IGIS in the case of assumed identities of ASIO officers) under sections 15LD and 15LE which have identified instances of wrongdoing or conduct that exceeds the limits of the relevant authority. In respect to reports made to the Attorney-General and the Commonwealth Ombudsman on controlled operations under sections 15HM, 15HN, 15HO, the Department refers the INSLM to the Commonwealth Ombudsman's annual reports on activities in monitoring controlled operations which are tabled in Parliament and published on the Commonwealth Ombudsman's website.

Questions 8-9: Experience with other Commonwealth disclosure offences applying to journalists

(8) Is the Department aware of any contraventions, or alleged or suspected contraventions, of disclosure offences other than section 35P by journalists, in connection with reporting on ASIO's activities or other national security operations? Please consider the following provisions and specified time periods in particular:

- **(a)** Section 34ZS of the ASIO Act in relation to questioning warrants and questioning and detention warrants (since the enactment of its predecessor, former 34VAA, in 2003).
- **(b)** Section 92 of the ASIO Act, concerning publication of the identity of ASIO officers. (Given the inclusion of this offence in the 1979 enactment, I would appreciate your suggestion as to a reasonable time period of consideration for present purposes. I may request further information if required.)
- **(c)** The official secrets offences in Part VII of the Crimes Act. (As with (b), I would appreciate your suggestion as to a reasonable time period of consideration for present purposes. I may request further information if required.)
- **(d)** The disclosure offences applying to delayed notification search warrants under section 3ZZHA of the Crimes Act (since the commencement of the scheme on 1 December 2014).

Proposed responses:

The Department is not aware of any contraventions, or alleged or suspected contraventions, of disclosure offences other than section 35P by journalists, in connection with reporting on ASIO's activities or other national security operations in respect of:

- section 34ZS of the ASIO Act;
- section 92 of the ASIO Act;
- the official secrets offences in Part VII of the Crimes Act; or

- the disclosure offences applying to delayed notification search warrants under section 3ZZHA of the Crimes Act.

The Department is aware of the use, or consideration of possible application of, some of these offences in a small number of cases. However the Department cannot recall any such matters in which journalists have been the subject of the action. However, the AFP, ASIO and / or the CDPP will be better placed to provide more comprehensive information about these matters.

(9) Is the Department aware of any contraventions, or alleged or suspected contraventions, by journalists or media organisations in relation to the recruitment advertisement offences in subsections 119.7(2) and (3) of the Criminal Code? (Noting that these provisions commenced on 1 December 2014, please also consider the predecessor to these provisions in section 9 of the now repealed *Crimes (Foreign Incursions and Recruitment) Act 1978.* Given the inclusion of section 9 in the original enactment of the 1978 Act, I would appreciate your suggestion of a reasonable time period of consideration for present purposes. I may request further information if required.)

Proposed responses:

The Department is not aware of any contraventions, or alleged or suspected contraventions, by journalists or media organisations in relation to the recruitment advertisement offences in subsections 119.7(2) and (3) of the Criminal Code, or in respect of the predecessor to these provisions in section 9 of the repealed *Crimes (Foreign Incursions and Recruitment) Act 1978* (which is, in effect, the same as the current offences in subsections 119.7(2) and (3) of the Criminal Code). However, as noted above, other agencies are likely to have more targeted records and information about these matters.

Questions 10-14: Legal policy, statutory interpretation and human rights compatibility matters
Section 35P of the ASIO Act

(10) In the Department's unclassified background briefing paper on section 35P provided to me on 21 January 2015, the Department provided comment on legal and legal policy issues concerning stakeholder suggestions for various amendments to section 35P. I would appreciate any further comments the Department may be able to provide on the following, additional materials raised in stakeholder commentary:

(a) It has been suggested that consideration be given to a new offence-specific defence to subsection 35P(1) pertaining to public interest disclosures made in good faith. It has been suggested that it would be possible to frame such a defence "in a manner which provides sufficient clarity [to persons making the disclosures], while still ensuring that information which is genuinely likely to result in serious harm to individuals is not publicly disclosed."

Can the Department provide any views on the feasibility or otherwise of framing a more limited or targeted public interest defence along the lines of this stakeholder suggestion?

Department's response

The Department considers it would be difficult to develop a workable offence-specific defence of public interest in good faith that would not undermine the efficacy of the SIO regime. The disclosure offences in subsections 35P(1) and (2) are based on the corresponding disclosure

offences in sections 15HK and 15HL of the Crimes Act in relation to controlled operations. Subsections 35P(1) and (2) are similarly subject to a number of exceptions (offence-specific defences) in subsection 35P(3), in addition to the general defences and excuses in Chapter 2 of the Criminal Code such as that of mistake or ignorance of fact (fault elements other than negligence). The exceptions in subsection 35P(3) substantially replicate the exceptions to the offences in sections 15HK and 15HL of the Crimes Act and include, for example, disclosures made in connection with the performance of the functions or duties, or the exercise of powers, of ASIO.

The question of whether there should be an additional exception for public interest disclosures was considered by the Parliamentary Joint Committee on Intelligence and Security (PJCIS). After considering relevant information and submissions on this matter, the PJCIS formed the view that such an additional exception was not desirable or necessary. The Committee reported that it:

> "paid close attention to concerns raised by inquiry participants about the potential impact of the proposed offences on press freedom. The Committee considers that in order to ensure the success of highly sensitive operations and to protect the identity of individuals involved, it is essential that information on these operations not be disclosed.
>
> However, the Committee also considers that it is important for this need for secrecy not to penalise legitimate public reporting. The Committee notes that, under the *Criminal Code Act 1995*, the fault element of 'recklessness' would apply to any prosecution of offences under proposed section 35P. This would mean that to be successful, the prosecution would be required by legislation to prove that a disclosure was 'reckless'. The structure of the offence provisions, as well as the requirement for the Commonwealth Director of Public Prosecutions to take the public interest into account before initiating a prosecution, provides an appropriate level of protection for press freedoms while balancing national security. However the Committee sees value in making these safeguards explicit in the Bill or the Explanatory Memorandum.
>
> The Committee considers that these safeguards, coupled with increased oversight by the IGIS over the issuing of SIOs, will provide appropriate protection for individuals, including journalists, who inadvertently make a disclosure of information about a current SIO. The Committee also highlights the important role of ASIO's existing 24-hour media unit in providing opportunities for journalists to clarify any concerns about a possible operation, including about the re-publication of any information."

The Government accepted the Committee's views on this issue and amendments were made to implement the Committee's recommendations.

The Department has considered the suggestion that consideration be given to a new offence-specific defence to subsection 35P(1) pertaining to public interest disclosure made in good faith, including in the various submissions to the inquiry,[1] and the suggestion that it would be possible to frame such a defence "in a manner which provides sufficient clarity [to persons making the disclosures], while still ensuring that information which is genuinely likely to result in serious harm to individuals is not publicly disclosed."

[1] The following submissions to the inquiry recommended a public interest defence: Seven West Media (represented by Addisons Lawyers), National Tertiary Education Union, Gilbert + Tobin Centre of Public Law, Professor Emeritus Clive Walker and Dr Matt Collins QC.

The Department remains of the view (as outlined in the joint AGD / ASIO public submission and in various submissions and responses to matters taken on notice to the PJCIS)[2] that the basic offence in subsection 35P(1) is designed to reflect that it is the disclosure of the very existence and conduct of a special intelligence operation that is the essence or gravamen of the offence. The offence in subsection 35P(1) is designed to deter those considering such a disclosure regardless of the profession, role or motivation of the discloser. Notwithstanding that a disclosure may be made in the public interest, and in good faith, it is the disclosure itself that creates an unacceptable risk that the operation may be compromised, and that the safety of the participants (and potentially their family or associates) may be jeopardised. The risk of harm may arise in both the immediate and longer term and the implications of the disclosure may not be fully understood by the discloser. The disclosure may also have unintended consequences where there is some connection between the SIO and another investigation.

The Department remains of the view that there are suitable mechanisms already available to journalists and members of the public to raise concerns about, for example, the conduct of ASIO, such as through the IGIS. This type of disclosure is already provided for as an exception or offence-specific defence to subsection 35P(1). When balanced against the possible harm that may be caused through the disclosure of the existence or conduct of an SIO in circumstances where the discloser may not be able to determine whether the information disclosed is genuinely not "likely to result in serious harm to individuals" either immediately or in the future, the Department considers that a public interest disclosure made in good faith offence-specific defence would seriously impact on the effectiveness of the SIO regime.

Any disclosures of information relating to an SIO (by a journalist, academic or any other person) would be considered in the context of all their particular circumstances, including the information disclosed and the circumstances in which the disclosure occurred in:

- the investigation of the disclosure pursuant to a possible contravention of subsection 35P (1);
- the context of determining whether to commence criminal proceedings in accordance with the *Prosecution Policy of the Commonwealth* which includes a public interest test; and
- the application of the CDPP's national legal direction and the Attorney-General's direction to the CDPP.

These kinds of measures recognise that there may be particular case-specific considerations relating to public interest that are appropriate to take into account in the application of the offences, but without creating an exception applying to particular segments of the community which would be contrary to criminal law policy and undermine the efficacy of the SIO regime.

The *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Data Retention Act) inserts new sections 180G and 180H into the *Telecommunications (Interception and Access) Act 1979* (TIA Act), requiring ASIO and law enforcement agencies to obtain a

[2] As outlined in the Attorney-General's Department and Australian Security Intelligence Organisation Joint Submission to this inquiry at pp. 10 -11 and 23-24; Attorney-General's Department's responses to matters taken on notice, Public Hearing of 15 August 2014 on the National Security Legislation Amendment Bill (No 1) 2014, p. 23; and the Attorney-General's Department's Second Supplementary Submission to the Parliamentary Joint Committee on Intelligence and Security Inquiry into the National Security Legislation Amendment Bill (No. 1), 8 September 2014, at pp. 7-8 and 13-14.

'journalist information warrant' in the very limited circumstances in which they wish to obtain telecommunications data for the purpose of identifying a journalist's confidential source of information. Before issuing a journalist information warrant the issuing authority must weigh the public interest involved in revealing the source's identity. The Department notes commentary (including in the context of submissions to this inquiry) that points to this extra protection for journalists in the Data Retention Act and the submission that a public interest disclosure in good faith exception should be included in the offence-specific defences in subsection 35P(3). The Department's view is that the protection accorded in the context of considering the public interest in the narrow context of disclosing a journalist's confidential source is quite different to the inclusion of an exception for journalists (or any class of person) in disclosing information relating to SIOs where the essence of the offence is the disclosure of the information itself and the risk of harm that results from that disclosure.

In the joint AGD / ASIO public submission to this inquiry, and in the context of commentary and submissions made to the inquiry by, for example the National Tertiary Education Union,[3] the Department notes that prosecutorial consent requirements are generally incorporated within the relevant offence provisions rather than by way of an executive order. The Department considers there could be benefit in including a general prosecutorial consent requirement in section 35P and that the requirement could apply to all prosecutions regardless of whether the alleged offender is a journalist, academic or any other person.

(b) It has been suggested that, notwithstanding the technical application of the elements of the 'basic offence' in subsection 35P(1), the absence of an explicit public interest or journalistic exemption may produce a 'chilling effect' on reporting of suspected wrongdoing by ASIO. Specifically, there is a suggestion that the offence is likely to create an incentive for journalists to take a conservative approach in the reporting of operational matters, rather than rely on the exercise of prosecutorial discretion. (For example, by electing not to report on some matters, or reporting very limited information.) It has also been suggested that section 35P may operate in combination with other disclosure offences in national security legislation to produce, in aggregate, a 'chilling effect' on journalists seeking to report on security matters.

Can the Department provide any comments to address these concerns, or to explain how they have been taken into account and balanced against other considerations in the framing of the elements of the offences in section 35P, particularly subsection (1)?

Department's response

The concerns raised about the absence of an explicit public interest or journalistic exemption in section 35P have been taken into account by the Government and balanced against other considerations, including that of the security and safety of participants in SIOs and the integrity of SIOs. These issues were considered in the framing of the safeguards, including in the way the elements of the offences were drafted, for example the inclusion of the fault element of recklessness in the context of the information disclosed relating to an SIO and that the person needs to have adverted to a substantial risk that the circumstance exists, the risk is unjustifiable

[3] National Tertiary Education Union Submission to this inquiry, p. 3.

and the person discloses the information anyway. The requirement that the CDPP takes into account the public interest before initiating a prosecution and that the Attorney-General's consent is required for prosecution proceedings to commence, provide additional safeguards.

There has been significant media reporting on counter-terrorism and security matters, including in the context of a number of trials. The Department has not seen any evidence of the suggested 'chilling effect' on reporting of law enforcement or security matters more broadly since the introduction of the various disclosure offences in the ASIO Act and the Crimes Act. Many of the disclosure offences have been in existence for many years and, to date, no journalists have been convicted of any of those offences. For example, in the context of the section 35P disclosure offences, similar disclosure offences in the controlled operations regime in the Crimes Act came into force in 2010 and no one has been prosecuted in relation to those offences. Neither has anyone been prosecuted in relation to corresponding disclosure offences in the controlled operations, assumed identities and witness protection legislation in State and Territory jurisdictions.

Journalists who have certain information are able to contact the ASIO media unit on a publicly listed number on ASIO's website which is staffed 24 hours each day to seek to verify information. Advice from law enforcement and security agencies is that media professionals have engaged effectively with them in seeking guidance or clarification about reporting on such matters, in order to avoid the risk of unintentionally compromising sensitive operations.

(c) Can the Department provide any comments on possible amendments to the elements of the offences? Please consider, in particular, the following possibilities:

- **(i)** Limiting the offences to the disclosure of certain types of information relating to a special intelligence operation. (For instance, limiting the offences to the disclosure of information that identifies a participant in an operation, or a method or technique utilised in the operation; or adopting the definition of 'operational information' in subsection 34ZS(5) of the ASIO Act, which applies to the disclosure offences in section 34ZS in relation to questioning warrants and questioning and detention warrants).
- **(ii)** Amending the phrase 'relates to' in paragraphs 35P(1)(b) and 35P(2)(b) to particularise the nature or degree of the relationship between the information disclosed and a special intelligence operation. (For example, would it be feasible, in the Department's view, to exclude information that relates to a special intelligence operation by way of identifying actions taken outside the authorised scope of a special intelligence operation?)
- **(iii)** Requiring the person disclosing the information to know that it relates to a special intelligence operation (as distinct from being reckless as to that relationship).

Department's response

The Department makes a general comment in respect of the three possibilities referred to in question 10(c) which is that it is the very disclosure of the existence and conduct of an SIO (regardless of what information is disclosed and by whom) that creates the risk that the operation may be compromised and that the safety of the participants (and potentially their family or associates) may be jeopardised. It is very likely that a potential discloser will simply not be in a position to know or to be able to predict the level of harm or consequences that may flow from a

disclosure. Such risks could be immediate, or arise over the longer term. The disclosure may also have unintended consequences where there is some connection between the SIO and another investigation.[4]

In respect of (i) limiting the offences to the disclosure of certain types of information relating to an SIO, for instance information that identifies a participant in an operation, or a method or technique utilised in the operation; or adopting the definition of 'operational information' in subsection 34ZS(5) of the ASIO Act, which applies to the disclosure offences in section 34ZS in relation to questioning warrants and questioning and detention warrants - aspects of these types of disclosure are already criminalised in the ASIO Act. For example, section 92 of the ASIO Act covers publishing the identity of an ASIO employee or ASIO affiliate, and section 79 of the Crimes Act covers the unauthorised disclosure of official secrets. These offences do not adequately reflect the nature of the harm caused by unauthorised disclosures of information in relation to an SIO, particularly prejudice to the operation itself, from disclosing the very existence and conduct of the operation.

Consideration could potentially be given to limiting the offences to the disclosure of information to that which indicates the existence of an SIO, the content of an SIO authority (including disclosing authorised conduct and participants, targets and other information about the satisfaction of the authorisation criteria) or the conduct of an SIO in accordance with an authority. However, the result could be that culpable conduct may go unpunished on the basis of a legal technicality rather than on the basis of the risk of harm. The risk of harm is arguably greater in relation to the disclosure of the existence of an SIO than in relation to questioning warrants and questioning and detention warrants. Those warrants authorise a single activity which is undertaken overtly (the questioning of a person before a prescribed authority), whereas SIOs are undertaken on a much larger scale, in a covert way, and over a considerably longer period of time. SIOs must remain covert, on an indefinite basis, to their targets and the wider community. Further, providing a greater degree of specificity in the physical elements of the offences in section 35P would increase the degree of difficulty in establishing the attendant fault elements, in particular establishing beyond reasonable doubt that the person was reckless as to the relationship between the information disclosed and the SIO. In light of all these issues, it is crucial for any consideration of possible amendments to the elements of the offences in section 35P that the potential operational impacts are explored in detail with ASIO, and practical enforcement implications are examined in consultation with the AFP and CDPP.[5]

In respect of (ii), the use of the phrase 'relates to' mirrors the wording in the controlled operations disclosure offences in sections 15HK and 15HL of the Crimes Act. The inclusion of the phrase 'relates to' has not been found to be too broad in that context, noting that no prosecutions have occurred in respect of those offences to date. Even if, as suggested in the submission made on behalf of Seven West Media,[6] it is feasible to exclude information that relates to an SIO by way of identifying actions taken outside the authorised scope of an SIO, the

[4] Attorney-General's Department and Australian Security Intelligence Organisation Joint Submission to this inquiry at p. 10.

[5] Attorney-General's Department and Australian Security Intelligence Organisation Joint Submission to this inquiry at pp. 26-27, 31-32; Attorney-General's Department's Second Supplementary Submission to the Parliamentary Joint Committee on Intelligence and Security Inquiry into the National Security Legislation Amendment Bill (No. 1), 8 September 2014, at pp. 7-8.

[6] Seven West Media (represented by Addisons Lawyers) Submission to this inquiry at pp. 12-13.

disclosure of such information may still jeopardise the operation, may jeopardise the safety of participants or their families and associates or may jeopardise related investigations. In the Department's view, the reporting and oversight mechanisms related to SIOs, as well as the ability of any person to report suspected wrongdoing on the part of ASIO to the IGIS, provide appropriate avenues for disclosure of actions taken outside the authorised scope of an SIO while, at the same time, mitigating the risk of harm associated with wider disclosure. In particular, we note the regular reports by the Director-General of ASIO to the Attorney-General and the IGIS on the conduct of SIOs in force, which must address the extent to which the SIO has assisted ASIO in the performance of one or more of its special intelligence functions, and must also specifically disclose whether the conduct of a participant in an SIO has caused death or injury, involved the commission of a sexual offence, or resulted in loss of or damage to property (section 35Q).

In respect of (iii), the physical element in (b) of each of subsections 35P(1) and (2) is a circumstance in which conduct occurs. As the provision does not specify a fault element for a physical element that consists of a circumstance, pursuant to subsection 5.6(2) of the Criminal Code, 'recklessness' is the fault element for that physical element. A person is 'reckless' with respect to a circumstance if he or she is aware of a substantial risk that the circumstance exists or will exist; and having regard to the circumstances known to him or her, it is unjustifiable to take the risk (subsection 5.4(1)).

If the fault element in respect of a circumstance is specified as 'knowledge', pursuant to subsection 5.3 of the Criminal Code, a person has knowledge of a circumstance if he or she is aware that it exists or will exist in the ordinary course of events (subsection 5.3).

In the context of proving the fault element of 'recklessness' as to the circumstance that the information disclosed by the person relates to an SIO, the prosecution has to establish beyond reasonable doubt that the person was aware of a substantial and not remote possibility that the information relates specifically to an SIO, and not just to an intelligence or national security related operation of some general description. Accordingly, the offences will not apply to a person who disclosed information entirely in the absence of an awareness that it could relate to an SIO, as there would be no evidence of an advertence to a risk of any kind.

SIO authorisations are entirely internal matters and this means that the burden on the prosecution to prove, beyond reasonable doubt, that the person was advertent to the risk that a specific circumstance existed, and that that risk was significant, is an onerous one.

In addition, the prosecution must further prove, beyond reasonable doubt, that having regard to the circumstances known to the person at the time of making the disclosure, it was unjustifiable to have taken that risk. Matters such as whether the person attempted to check facts and consult with ASIO about the potential disclosure of the information, would be factors taken into account in assessing whether the prosecution could establish the requisite fault element.

The policy justification for adopting recklessness, rather than knowledge, as the applicable fault element is that the wrongdoing targeted by the offences in section 35P - the disclosure of information about the existence of an SIO - will, by its very nature, create a significant risk to the integrity of that operation and the safety of its participants. The fault element of recklessness gives expression to the policy imperative to deter such conduct by clearly placing an onus on the

person contemplating the public disclosure of information relating to an SIO to consider whether there is a substantial risk that the information relates to an SIO and, if so, whether it is justifiable, at law, to take the risk of disclosing information that relates to an SIO.[7]

(11) This question relates to the scenario in which a journalist who is concerned that a potential report on an operational matter may contravene subsection 35P(1) because it may contain information that relates to a special intelligence operation, and seeks information from ASIO's media liaison unit about this matter.

(a) Does the Department consider that the offence in subsection 35P(1) could potentially apply to an ASIO officer who provides information to a journalist in response to such an enquiry in these circumstances?

(b) Are the defences in paragraphs 35P(3)(a) or (d) intended to apply to these circumstances? If so, please provide an explanation of their intended operation.

Department's response

The Department considers that an offence in subsection 35P(1) is not likely to apply to an ASIO officer who provides information to a journalist in response to an enquiry about whether information the journalist is considering disclosing relates to an SIO. In accordance with the exemptions to the offences in section 35P outlined in subsection 35P(3), the offences do not apply if the disclosure of information by the ASIO officer to the journalist was (a) in connection with the administration or execution of Division 4 of Part III of the ASIO Act; or (d) in connection with the performance of functions or duties, or the exercise of powers, of ASIO. The exemptions give effect to a policy position that disclosures of information relating to SIOs are primarily and appropriately made by internal means, that is by ASIO to, for example, the IGIS, rather than via indiscriminate, public means.

An ASIO officer's conduct in disclosing information to a journalist in the context of the journalist's proposed disclosure of information potentially relating to an SIO, and likewise engaging effectively with a journalist in providing guidance or clarification about reporting on such matters, in order to avoid the risk of unintentionally compromising sensitive operations, falls within the ambit of the exemptions to the offences in section 35P outlined above (for example pursuant to subsection 17(1)(b) of the ASIO Act and the communication of intelligence (subsection 18(1)). This is so particularly in circumstances in which the Director-General of ASIO has provided clear authorisation for such engagement with the journalist in the context of the matters referred to above.

(12) Does the Department have any views on whether the inclusion of the notes to subsections 35P(1) and (2), with respect to the fault element applying to each of paragraphs 35P(1)(b) and 35P(2)(c), may have any implications for the interpretation of the fault element applying to paragraph 35P(2)(c)? That is, could the absence of a corresponding note to paragraph 35P(2)(c) give rise to a credible argument that there is a necessary intendment to displace the default fault element of recklessness under section 5.6(2) of the Criminal Code?

[7] Attorney-General's Department and Australian Security Intelligence Organisation Joint Submission to this inquiry at p. 27, citing the Attorney-General's correspondence to the Senate Scrutiny of Bills Committee.

Department's response

The notes to subsections 35P(1) and (2) were inserted into the provisions in response to recommendation 13 of the PJCIS in its inquiry into the Bill. The purpose of the insertion of the notes with respect of paragraphs (1)(b) and (2)(b) was, in light of particular queries and concerns that had been raised about those particular provisions, to confirm that the fault element of recklessness applies to the circumstance that the information relates to an SIO, pursuant to subsection 5.6 of the Criminal Code. The Department notes the observations made about this issue in the submission made on behalf of Seven West Media and makes the following comment.[8] The absence of a corresponding note in respect of paragraph 35P(2)(c) does not have any implications for the interpretation of the fault elements applying to that paragraph which are 'intention' in respect of paragraph 35P(2)(c)(i) as specified within the provision and 'recklessness' in respect of paragraph 35P(2)(c)(ii), by virtue of subsection 5.6(1) of the Criminal Code .

While it is not considered necessary to include notes of this kind due to the ordinary operation of the Criminal Code, various notes have been inserted in a range of criminal offences in the Criminal Code (and other legislation) to provide clarity and to assuage concerns where provisions have been the subject of considerable scrutiny and public attention. This does not affect the ordinary application of the Criminal Code to other offence provisions.

(13) In its Sixteenth Report of the 44th Parliament, the Parliamentary Joint Committee on Human Rights concluded that section 35P is incompatible with the right to freedom of expression under Article 19 of the International Covenant on Civil and Political Rights. The Committee was not satisfied that the offences were demonstrated to be a reasonable, necessary or proportionate limitation on that right.

Can the Department outline the basis upon which the Government is satisfied that section 35P is compatible with the right to freedom of expression, having particular regard to its application or potential application to journalists and others seeking to reports matters in the public interest, such as suspected wrongdoing in the course of special intelligence operations?

Department's response

The Department considers the offences in section 35P are a permissible limitation on the right to freedom of expression in Article 19(2) of the *International Covenant on Civil and Political Rights* on the basis of the offences being reasonable, necessary, and proportionate to the achievement of a legitimate objective. The Committee acknowledged, in the context of consideration of the right to privacy, that the maintenance of national security and protection of the Australian community may be regarded as a legitimate objective.

The offence provisions in section 35P are necessary to achieve the legitimate objective of protecting persons participating in an SIO, for example an ASIO operative infiltrating a terrorist organisation, and to ensuring the integrity of such operations, by creating a deterrent to unauthorised disclosures of information about their existence or methodology, which may place at risk the safety of participants or the effective conduct of the operation.

[8] Seven West Media (represented by Addisons Lawyers) Submission to this inquiry at p. 10.

The offence provisions are rationally connected to the legitimate objective they pursue. The offences will help to ensure the integrity of SIOs and protect persons participating in them by creating a deterrent, in the form of a criminal sanction, to disclosing information that may place these operations or their participants (or family members or associates) at risk. A criminal sanction is appropriate, having regard to the gravity of the risks presented by the disclosure of the existence of an SIO – noting that such risks do not depend on the motives of the discloser, nor diminish with the passage of time, and that such risks are not capable of being averted or adequately managed once a disclosure is made. It is therefore appropriate that all members of the community are subject to a non-disclosure duty in relation to such operations.

The provisions are also proportionate to achieving the legitimate objective. Both offences in section 35P are subject to all of the general defences and excuses in Chapter 2 of the Criminal Code. In addition, they are subject to administrative safeguards and specific exceptions (which operate as offence-specific defences) contained in subsection 35P(3). Importantly, the offences in section 35P only apply to persons who disclose information reckless as to the circumstance of its relationship to an SIO – that is, awareness of a substantial risk that the information relates to not merely to any type of intelligence collection operation, but specifically one that is authorised and conducted under the provisions of Division 4 of Part III. The prosecution must prove, beyond reasonable doubt, that the person was aware of a real and not remote possibility of this very specific connection, and nonetheless and unjustifiably, in the circumstances known to him or her at the time, disclosed the information. The level of specificity required, together with the high standard of proof, and the fact that SIOs are authorised and conducted on a solely internal basis, makes this a very difficult requirement to satisfy, such that prosecutions are anticipated to be very rare.

Since 2010, offences with identical elements have existed in the controlled operations scheme in Part IAB of the Crimes Act (sections 15HK and 15HL). There have been no investigations or referrals for prosecution in relation to these offences. This strongly suggests that concerns about limitations on freedom of expression have not been substantiated in practice. In addition, corresponding disclosure offences (with identical elements) exist in the controlled operations, assumed identities and witness protection legislation of nearly all jurisdictions. The disclosure offence was developed and agreed to by all Governments as part of a model national law on cross-border investigative powers in 2003.

A comprehensive analysis of the compatibility of section 35P with Article 19 of the ICCPR is provided at **Attachment A**.

Disclosure offences in the model national laws for cross-border investigative powers

Question (14) relates to the disclosure offences applying to the model national laws for controlled operations, assumed identities and witness protection for law enforcement operatives, as developed by a Joint Working Group (JWG) established by the former Standing Committee of Attorneys-General (SCAG) and the former Australasian Police Ministers Council (APMC) in 2002-2003, and later endorsed by first ministers.

(14) The 2003 discussion paper and report of the JWG on the model national laws do not appear to document consideration of the potential application of the disclosure offences to journalists or members of the media. Noting that a staff member of the Department chaired the JWG and that

the membership included several Departmental officers, does the Department have any information about, or recollection of, whether specific consideration was given to this matter in the course of the JWG's work (or in any subsequent consideration by relevant ministerial bodies) and if so, to what effect?

Department's Response:

The Department has identified and spoken with a number of current and former Departmental officers who were involved in the work of the JWG, including the development of the discussion paper and report of the JWG on the model national laws. Those officers had no information about, or recollection of, specific consideration being given to the potential application of the disclosure offences to journalists or members of the media.

Questions 15-19: Arrangements for media reporting of national security operations

I am aware that in May 2011, the (then) Attorney-General, the Hon Robert McClelland MP, circulated a set of overarching principles to major Australian media organisations concerning the reporting of matters involving potentially sensitive national security and law enforcement information.

I understand that these principles reflected matters agreed between representatives of those media organisations and the Attorney-General at a round-table discussion in April 2011. I understand that a key outcome was that the Department would provide media organisations with a list containing key law enforcement and security agency contacts who would be available to receive media inquiries 24/7, and that media organisations would similarly provide the Department with appropriate contacts for distribution to law enforcement and security agencies.

The following questions relate to the status and application of the principles and arrangements.

(15) To the Department's knowledge, do the principles and arrangements remain agreed by the media organisations to which they were circulated, and any other media organisations to which they may apply?

(16) The principles indicate that the agreed media communications and liaison arrangements apply to persons who are 'professional journalists'. Is there a common, intended meaning of this term? Or, alternatively, is it a matter for the discretion of individual security or law enforcement agencies? Please include a brief explanation of the policy reasons for the intended meaning or approach to the interpretation of this term.

(17) Have the principles or media liaison arrangements been revised on a whole –of- Government basis since May 2011? Has consideration been given to doing so, or is it contemplated that consideration may be given to doing so, having regard to developments such as recent amendments to disclosure offences in security legislation, and changes in the security environment and media organisational or business practices?

(18) The principles indicate that, if there are any concerns that the arrangements are not being implemented properly, any such issues should be raised with the Department. Have media organisations raised any concerns with the Department, particularly with respect to the operation of the arrangements in relation to journalists who may be concerned that they could potentially disclose operationally sensitive information and be subject to criminal liability?

(19) I understand that there was some suggestion in 2011 to hold further round-table discussions with the media about the reporting of national security matters, to provide an opportunity for ongoing

dialogue about the arrangements. Has the Department hosted subsequent round-tables or undertaken other forms of liaison for this purpose? Please include a brief explanation of reasons for this position. If further liaison has been undertaken, please provide details of the matters discussed and their outcomes.

Department's Response:

15 (and 17). The round-table chaired by the then Attorney-General in April 2011 provided an opportunity for senior representatives from media organisations and Commonwealth and State government and law enforcement agencies to discuss the continuing need for open and clear communication between media and law enforcement agencies in the context of reporting on matters involving potentially sensitive national security and law enforcement information. One of the outcomes of the round-table was an agreed set of overarching principles:

- the overriding importance of preventing harm to the public and operational security and law enforcement personnel;
- the preservation of freedom of speech and editorial independence;
- the requirement for the protection of sensitive security and law enforcement information, including in order for security and law enforcement agencies to effectively conduct their operations; and
- the inherent public interest in news relating to security matters.

The Department subsequently collaborated with media organisations, law enforcement and security agencies to develop a 24/7 contact list to be used when dealing with the publication of information that is potentially sensitive from a law enforcement or national security perspective. The list was distributed to key law enforcement, security and media contacts in September 2011.

The principles set out above, which are overarching and broad, continue to underpin the communication between media organisations who interact with the Department, and security and law enforcement agencies on a regular basis about potential and actual sensitive national security and law enforcement information. The established contact arrangements also continue to apply between media organisations and the Department and security and law enforcement agencies, which are available on a 24/7 basis.

16. The definition of 'journalist' has been the subject of ongoing and more recent discussion in the context of the passage of the National Security Legislation Amendment Bill (No.1) 2014 (NSLAB 1) and the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015. In the Final Report of the PJCIS on NSLAB 1 the Committee made the following comment about the difficulty of defining the term 'journalist':

> "Taking these safeguards into account, the Committee does not consider it appropriate to provide an explicit exemption for journalists from the proposed offence provisions. Part of the reason for this is that the term 'journalism' is increasingly difficult to define as digital technologies have made the publication of material easier. The Committee considers that it would be all too easy for an individual, calling themselves a 'journalist', to publish material on a social media page or website that had serious consequences for a sensitive intelligence operation. It is important for the individual who made such a disclosure to be subject to the same laws as any other individual" (at p.62).

The concept of a 'journalist' is considered in the Revised Explanatory Memorandum to the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015 in the context of the inclusion of the journalist information warrant in Chapter 3 of the TIA Act:

> "The concept of a 'journalist' is intended to replicate the current approach in Division 119 of the Criminal Code, as amended by the *Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014*. Subsection 119.2(3)(f) of the Criminal Code provides that where a person is working in a professional capacity as a journalist, or is assisting another person working in a professional capacity as a journalist, they are exempted from the general prohibition from entering or remaining in, a declared area. Similarly, an individual is a journalist under Division 4C if they are working as a journalist in a professional capacity. Indicators that a person is acting in a professional capacity include regular employment, adherence to enforceable ethical standards and membership of a professional body" (at p.78).

The above may provide some guidance as to the Government's perspective on the meaning of the term 'journalist', albeit in the specific contexts of the exemption from the general prohibition from entering or remaining in a 'declared area' and in the requirement for obtaining a 'journalist information warrant'. As outlined above in response to question 10(a), the Department remains strongly of the view that a public interest in good faith exception for journalists (or any class of person) is not in line with the framework of the disclosure offences in section 35P of the ASIO Act, where the essence of the offence is the disclosure of the information itself and the risk of harm that results from that disclosure.

18. No concerns have been raised by media organisations with the Department about arrangements not being implemented properly flowing from the 2011 round-table and the agreed overarching principles. This includes in respect of the operation of the arrangements in relation to journalists who may be concerned that they could potentially disclose operationally sensitive information and be subject to criminal liability.

19. There was some suggestion in 2011 to hold further round-table discussions with media organisations about the reporting of national security matters and to provide an opportunity for ongoing dialogue about the arrangements. However, given that the media arrangements in place following the round-table were considered sufficient and that no concerns were raised by media organisations with the Department about the arrangements not being implemented properly, the need to continue the discussions in a round-table form dissipated.

The communication between the Department and media organisations has continued to adapt to changes in the security environment. In July 2013 the Department organised a round-table attended by senior media representatives and community leaders to discuss the role of language in countering terrorism and violent extremism and how public language can be used to challenge extremist narratives used to recruit vulnerable youth. A *Talking about Violent Extremism* language guide was distributed and media representatives undertook to share the guide internally.

The Department also continues to engage with the media on particular issues as the need arises.

The Department's response to an issue raised in the submissions – sunset provisions.

Many of the issues raised by submitters to the inquiry are addressed in the Department's responses to the INSLM's specific questions above.

However, an additional issue is raised in the submission made on behalf of Seven West Media and, tangentially in the submission made by Dr Matt Collins QC, in respect of the inclusion of a sunset provision to the section 35P disclosure offence provisions.

As outlined in the AGD/ ASIO joint submission into the inquiry at page 28, AGD and ASIO made comments in relation to application of sunset provisions to the provisions to the PCJIS inquiry into the (then) Bill:

> "The Department and ASIO do not support the application of a sunset provision to the provisions in Schedule 3 to the Bill. The need to provide participants in covert intelligence operations with limited protection from legal liability is not temporary in nature. Rather, its ongoing availability is needed to ensure that the Organisation has the capacity to meet emerging and future security challenges, by ensuring its capacity to gain close access to persons and groups of security concern, and providing legal certainty to persons assisting the Organisation in the performance of its functions.
>
> The permanent nature of a special intelligence operations regime is consistent with the controlled operations scheme in Part 1AB of the Crimes Act, and the immunity from liability conferred upon staff members and agents of Intelligence Services Act agencies under section 14 of that Act. Both of these measures were enacted without sunset clauses, and this was found acceptable to the Parliament in 2010 and 2001 respectively."

The Department will provide any additional information on these or other issues raised in the context of the inquiry and public and private hearings as required.