ASIO response to request for information regarding the Acting Independent National Security Legislation Monitor's inquiry into section 35P of the ASIO Act

ASIO provided a complete response to each of the questions posed by the Acting Independent National Security Legislation Monitor. Portions of that response were classified and have been removed as their release may prejudice national security.

Please describe ASIO's media liaison arrangements with respect to journalists or other media professionals who may contact ASIO about matters that may relate to operational activities. I am particularly interested in details of the following:

a. ASIO's approach to the handling of inquiries from journalists who may contact its media liaison unit in relation to a potential news report or editorial piece because they are uncertain whether it may disclose operationally sensitive information (and may further be concerned about exposure to criminal liability if the relevant report was published and, in fact, disclosed such information)

Media inquiries received by ASIO are managed in accordance with standard operating procedures. To perform its statutory functions, ASIO must employ a conservative approach to media engagement with respect to operational matters. ASIO does not confirm details relating to individuals, investigations or operations as a matter of course. This includes inquiries in relation to special intelligence operations or other operationally sensitive information.

If journalists contact ASIO Media regarding an operational matter they intend to report on, ASIO advises the relevant line-area within the Organisation before responding to the journalist. When ASIO has concerns about the sensitivities around the subject being reported on, ASIO does not provide a public comment, but may decide to speak with the journalist on a confidential basis to provide context on that sensitivity. In this instance, the journalist may be contacted by the Director-General or a Deputy Director-General to explain how Australia's national security would be prejudiced if the subject was reported on publicly.

All media inquiries, and responses, are logged and retained for accountability and future reference.

Management of 35P

ASIO's approach to handling media inquiries where the subsequent media coverage may disclose information related to a special intelligence operation—potentially in contravention of section 35P—is determined on a case-by-case basis. The following objectives are considered:

- The protection of the identity and safety of ASIO human sources or employees.
- The protection of public safety.
- The protection of ASIO capabilities and methods of operation.

- The protection of the ongoing effectiveness of the particular special intelligence operation, or any other operations, which could be adversely impacted by compromise of the special intelligence operation.

ASIO accepts that its response to a journalist in relation to an inquiry regarding a special intelligence operation, including 'no comment', may be relevant to whether there has been any contravention of section 35P and indeed whether a prosecution would be in the public interest.

b. any practices ASIO has implemented to manage the risk of confirming or denying the existence of a covert operation, in the event a journalist contacted ASIO's media liaison unit in the circumstances described at (a) above

The existing method of handling media inquiries, as noted above, addresses the risk of confirming or denying the existence of a covert operation.

c. whether there are any specific arrangements in place, or under consideration, with respect to liaison with journalists who may contact ASIO in relation to prospective news or editorial reports, out of concern that they may disclose information relating to a special intelligence operation, potentially in contravention of section 35P

Any proposal to provide, deny, or confirm sensitive operational information for the purpose of assisting a journalist to understand the potential for a proposed disclosure to contravene section 35P would be balanced against the objectives stated above.

The existing method of handling media inquiries, as noted above, addresses concerns related to the disclosure of information related to a special intelligence operation. Media inquiries regarding special intelligence operations are determined as per inquiries about investigations or operations—and therefore would not receive a public comment.

In practice, if a journalist approached ASIO for comment on information they believed to be operationally sensitive, and which ASIO knew to be related to a special intelligence operation, ASIO would consider speaking with the journalist on a confidential basis to explain the sensitivities of the information. A number of considerations would go to determining whether to inform the journalist of the existence of a special intelligence operation, including whether a person might be harmed should the existence of a special intelligence operation be revealed. If, after receiving a confidential briefing by ASIO, the journalist still intended to publish the information, ASIO would advise the journalist that to do so may breach 35P. It would then be for the journalist to decide whether or not to proceed with publishing the information.

d. how, if at all, 'journalists' and 'media organisations' (or similar descriptors) are defined or otherwise interpreted by ASIO for the purpose of its media liaison activities. (For example, are there circumstances in which ASIO might decline to liaise with a person who self-identified as a journalist, or an entity that described itself as a media organisation, but did not satisfy ASIO's interpretation?)

ASIO defines journalists and media organisations as accredited individuals or entities of media or news organisations.

ASIO Media staff have extensive knowledge of the media industry and professional training and experience in journalism and/or public affairs. The majority of journalists are already known to ASIO Media as a result of previous official interaction.

Each media inquiry is carefully considered and scrutinised for legitimacy. Even if an inquiry appears to originate from an unaccredited media representative (for example, a university student), ASIO may still comment. All comments, once made, are on the public record.

Organisation's experience with respect to other disclosure offences applying to journalists

ASIO records do not show any instances where journalists were investigated internally, or referred to law enforcement agencies, for suspected contraventions of disclosure offences under sections 34ZS or section 92 of the ASIO Act, section 15LC of the *Crimes Act 1914* (Crimes Act), or the official secrets offences in part VII of the Crimes Act.

Identification of suspected incidents of wrongdoing in relation to the use of assumed identities by ASIO officers

ASIO examined its reports to the Inspector-General of Intelligence and Security (IGIS) under section 15LE of the Crimes Act made between 2008 and 2014, and found no fraud or any other unlawful activity under section 15LG.

Potential amendments to elements of the offences and offence-specific defences.

a. **It has been suggested that consideration could 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 disclosures], while still ensuring that information which is genuinely likely to result in serious harm to individuals is not publicly disclosed". Can ASIO provide any views on the feasibility or otherwise of framing a defence in this way?**

ASIO strongly recommends against the inclusion of a specific public interest disclosure defence to subsection 35P(1).

Because the disclosure of information about a special intelligence operation will create—at the very least—a significant risk of prejudice to the operation and the safety of its participants, a specific public interest defence is not appropriate.

ASIO therefore regards the absence of a public interest defence, and hence the encouragement for anyone considering making a disclosure to do so under the *Inspector-General of Intelligence and Security Act 1986* (IGIS Act) and the *Public Interest Disclosure Act 2013* (PID Act) as appropriate.

Even where a person makes, in good faith, a disclosure based on *their understanding* of the application of a public interest defence, they may inadvertently disclose information prejudicial to the special intelligence operation and its participants. Any resultant harm would be incurred regardless of the intention of the disclosing individual or the outcome of any subsequent prosecution.

For example, a person may be able to use information (seemingly innocuous to the discloser), to complete an intelligence picture which identifies the existence or intent of an operation or the identity of participants. This mosaic effect makes it very difficult to frame a defence in a manner which would provide sufficient clarity to persons intending to make a disclosure, while still ensuring that information which is likely to result in prejudice to an operation or the safety of persons involved is not disclosed. Where the person using the information to complete that picture is, or is associated with the target of the special intelligence operation, the participants in that operation will be at significant risk of physical harm. For example, retribution could be threatened against an ASIO source, or their family, if the source's role with ASIO was discovered.

The ASIO Act enables all persons, including public officials, to make public interest disclosures in relation to special intelligence operations to the IGIS. The IGIS Act and the PID Act were designed to enable public interest disclosures relating to security and intelligence matters to be made and addressed in such a way so as to not prejudice security or the safety of any person. The IGIS has powers similar to that of a royal commission in relation to ASIO and may compel the production of

information and the giving of sworn evidence. Failure to comply with those demands is an offence.[1] The IGIS may also enter any place occupied by a Commonwealth agency for the purposes of an inquiry.[2]

If a disclosure is made under the PID Act there are protections from civil, criminal or administrative liability, protection of the discloser's identity and protection from reprisal. These protections are available even if the discloser's report of wrongdoing turns out to be incorrect, provided at the time of the disclosure the provider reasonably believed the information tends to show disclosable conduct as defined under the PID Act.

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 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 prosecutorial discretion not to enforce an offence. (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 ASIO provide any comments to address these concerns, or to explain how they have been taken into account and balanced against other interests in the framing of the elements of the offences in section 35P, particularly subsection 35P(1)?**

ASIO strongly contends that section 35P, itself or in concert with other disclosure offences, should not produce a 'chilling effect' on reporting of suspected wrongdoing.

The offence will not, and is not designed to, criminalise legitimate reporting. However, while there is a strong public interest in maintaining public awareness of government wrongdoing, there is a corresponding public interest in protecting national security and the safety of persons working on behalf of their country and fellow citizens to keep them safe. The framing of subsection 35P(1) reflects this—it is directed at the harm which may arise from the unauthorised disclosure of information relating to a special intelligence operation which occurs regardless of the location, motives or profession of the discloser.

ASIO undertakes its activities for the purposes of security, which, in essence, is the protection of Australia and its people from threats designated by Parliament as security risks. The disclosure of information relating to ASIO's activities therefore has the potential to prejudice security or the safety of persons involved in the performance of ASIO's functions and their associates. As such,

[1] Section 18 of the IGIS Act
[2] Section 19 of the IGIS Act

the normal practices of responsible journalism are key to ensuring any disclosures made are in the public interest (both in exposing government wrong doing and in protecting Australia and its people from security threats) and not merely *of* public interest.

ASIO refers to advice provided in the joint ASIO-AGD public submission to your inquiry that, for the offence to apply to a journalist reporting on national security matters, the journalist would need to be aware of a substantial risk that the information related to a special intelligence operation and nonetheless and unjustifiably in the circumstances known to him or her at the time, took that risk and communicated the information. In assessing whether a person's conduct was justified, any steps the person takes to mitigate that risk will be a relevant consideration, for example checking facts and, if in doubt, consulting ASIO. ASIO engages with the media on a range of issues and has a 24-hour media unit (discussed above) with which a journalist may engage to clarify any concerns.

Furthermore, where there is an instance of suspected wrongdoing a person, including a journalist, may refer it to ASIO or to the IGIS (as discussed above). Along with reporting to the Attorney-General and the IGIS, ASIO may communicate information relating to a serious offence[3] to the relevant Commonwealth, State or Territory authority. The IGIS may also refer any matter involving criminality to the relevant law enforcement agency. This provides a mechanism for matters of public interest (the investigation of alleged government wrong doing) to be adequately addressed without the risk of prejudice to security or to safety that may arise from a disclosure.

Given the necessarily covert nature of special intelligence operations, the unauthorised disclosure of related information heightens the risk of prejudice to the operation, to the safety of persons involved and to security more broadly. For example, in addition to the risks posed by the persons being investigated and their associates, there is also a risk posed by entities with analogous hostile intentions. Such entities could use knowledge obtained to protect their own activities, and to expose ASIO's methods, capabilities and staff. This would enable foreign intelligence services to target ASIO employees or affiliates and to frustrate the performance by ASIO of its statutory functions.

As Justice Hope observed in his 1984 report on ASIO, "*the disclosure of secrets or the exposure of secure areas to risk through inadvertence or carelessness can result in just as much damage to the national interest as can result from espionage or sabotage*". Further, the damage caused to national security by an unauthorised disclosure may not always be readily apparent or easily proved or it may take a significant period of time for the negative effects of a disclosure to be properly understood and quantified (especially as foreign intelligence services also act in secrecy).

The motives of a discloser could seriously increase the resultant harm, which is why a tiered offence regime is necessary to reflect the greater level of culpability that would attach to a person who intended to cause harm by his or her disclosure. It would be open to a sentencing court to

[3] Serious offence is defined in section 4 of the ASIO Act as being an offence punishable by more than 12 months imprisonment

determine an appropriate penalty, in accordance with general sentencing rules and having regard to the circumstances of individual cases.

The offences in section 35P are modelled on the existing offences in section 15HK and section 15HL of the Crimes Act in relation to controlled operations by law enforcement agencies. ASIO understands the AFP has advised there have been no prosecutions or referrals for prosecution in relation to section 15HK and section 15HL since their enactment in 2010. Given the significant volume of controlled operations that have been authorised since 2010, the lack of any prosecution for these offences, whether of journalists or otherwise, suggests the offences have not had a 'chilling effect' on the reporting of law enforcement activities.

c. Can ASIO 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).

ASIO opposes limiting the physical element of the offences to the disclosure of certain types of information. Such a change would result in section 35P no longer according with the harm, or significant risk of harm, inherent to the disclosure of *any* information relating to a special intelligence operation, and would increase— disproportionately— the degree of difficulty in establishing the attendant fault elements of 35P.

Under section 35P, the prosecution must prove a person was reckless as to the particular type of relationship between the information disclosed and the special intelligence operation. The more narrowly or specifically that circumstance is prescribed in the physical elements of the offence, the greater the possibility for reasonable doubt to exist—especially in relation to the attendant fault elements. This may produce the unintended consequence that conduct that should properly be regarded as culpable (due to the risk it presents of operational compromise or harm to participants) may go unpunished on the basis of a technicality as to the particular nature of the relationship between the information disclosed and the special intelligence operation (and the discloser's awareness of that relationship).

The likelihood of a prosecution succeeding also directly contributes to the balancing of whether bringing a prosecution is in the public interest compared to the harm to national security and the safety of participants that would be caused by confirming the accuracy of any unauthorised disclosure. If the offence provision is drawn too narrowly it lessens the likelihood of a successful prosecution for an unauthorised disclosure and therefore lessens the likelihood that the

wrongdoer will be brought to account because of the attendant national security and safety considerations of bringing a prosecution.

With specific respect to adopting the definition of 'operational information' in subsection 34ZS(5) of the ASIO Act, the risk of harm in relation to the disclosure of the existence of a special intelligence operation (or any other information that may compromise its effective conduct) is arguably greater than that which may arise in relation to questioning warrants and questioning and detention warrants as those warrants authorise a single activity (namely coercive questioning of an individual). Although the dissemination of information relating to questioning warrants and questioning and detention warrants needs to be contained to ensure their effectiveness, unlike a special intelligence operation they are not a covert means of investigation as the person being questioned is aware he or she, or persons connected with him or her, are of security interest to ASIO. Special intelligence operations are undertaken on a much larger scale and run over a considerably longer period of time. They must remain covert, on an indefinite basis, to their targets and the wider community as it could, for example:

- Jeopardise the ongoing investigation into the security threat that was the subject of the special intelligence operation;
- Jeopardise other investigations where there is some connection between the two, for example:
    - if there is some relationship between the persons being investigated; or
    - an authorised participant, whose identity is able to be inferred, is known to associate with other persons who are also performing investigative roles;
- Jeopardise other investigations in which a pattern of operational activity is being employed that is similar to that disclosed;
- Lead to the identification of an authorised participant and subsequent reprisals against them and their family or associates, even where a participant is deceased;
- Lead to the identification of ASIO staff, methods and capabilities which will render ASIO more susceptible to the activities of foreign intelligence services;
- Lead to the identification of ASIO staff which may subject them to heighted risk to their personal safety.

The categories of information included in section 34ZS would be insufficient to protect the public interest in the ongoing investigation of the security threat which was the subject of the special intelligence operation. Section 34ZS divides information into essentially two categories: 1) information relating to the fact that a warrant has been issued, the content of the warrant and actions taken under the warrant (that is, questioning and/or detention of a person); and 2) operational information. Subsection 34ZS(5) defines ‘operational information’ to mean information indicating: information ASIO has or had; a source of information ASIO has or had; or an operational method, capability or plan of ASIO.

This division suggests that the information in the first category may not be operational information (especially because those aspects are overt). If the definition of operational information in section 34ZS were used, it may imply a special intelligence operation has been

authorised and actions taken under that authority are not protected by the unauthorised disclosure offence. This may lead to the exposure of covert ASIO investigation of security threats or at least of sufficient information from which ASIO investigative interests could be inferred. Where investigative targets become aware of, or suspect, security (or law enforcement) interest in their activities or gain knowledge of the methods employed by investigative agencies, they change their behaviour to make their conduct less detectable to authorities. The result is that it becomes more difficult for ASIO to collect intelligence relevant to security and protect Australia from security threats, or to prevent those threats from materialising without adequate forewarning.

Further, in categorising information it must be remembered that, in an intelligence context, it is not just information that identifies a participant or a particular method or technique, but also information which, when used with other information, may lead a person to suspect that that a special intelligence operation is being conducted, or that a particular person may be a participant or ASIO employee or affiliate, or that a particular activity or person is of security interest. Intelligence agencies (including foreign intelligence agencies) specialise in putting together seemingly harmless and meaningless pieces of information to create a picture or a partial picture of the matter they are investigating. Non-State actors and individuals have also been known to employ this technique. While a single piece of information may not immediately disclose (for example, the identity of a participant), over time as more individual pieces of information are released or otherwise obtained, they will be able to be put together like pieces of a puzzle to enable that identification to take place.

ii. Amending the phrase 'relates to' in paragraphs 35P(1)(b) and 35P(2)(b) to particularise the nature or degree of relationship between the information disclosed and a special intelligence operation. (For example, would it be feasible, in ASIO'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?)

ASIO does not consider it feasible to limit the term “relates to” in paragraphs 35P(1)(b) and 35P(2)(b) to exclude actions taken outside of the scope of the authority. This is because the protection of the existence of a special intelligence operation and ASIO’s investigative interests would still likely need to be maintained. For example, should the actions of one participant result in serious injury to a person, it does not automatically justify the disclosing of the investigation to the broader public such that it could result in a loss of coverage of a security threat or lead to the identification of other persons (who were not involved in that conduct) as participants which would then prejudice that person’s safety. Therefore any attempt to exclude particular types of information from the application of section 35P should be approached cautiously so that the very significant public interests in maintaining an investigation into a security threat and protecting the safety of innocents is not prejudiced.

Unlawful conduct outside the scope of a special intelligence operation authority would give rise to criminal and civil liability for that conduct. Unlawful conduct may be investigated by relevant law

enforcement agencies regardless of whether or not a special intelligence operation was, or is, in existence.

ASIO must report to the Attorney-General and the IGIS any conduct involved in a special intelligence operation which results in death or injury to any person, involves the commission of a sexual offence, or loss of or damage to, property. The Attorney-General or the IGIS may call for, or conduct an inquiry into, the actions taken under a special intelligence operation and may refer unlawful conduct to law enforcement agencies for investigation. Where any referral to law enforcement agencies results in a prosecution, there is a defence for the reporting of legal proceedings so any disclosure of a special intelligence operation in open court would be able to be reported on (subject to any court orders).

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).

ASIO does not support a fault element of knowledge as it would be unduly onerous to prove this fault element in the course of a prosecution and a fault element of recklessness would encourage an individual to contemplate the nature of the information they are considering disclosing and the implications of its release.

Section 5.4 of the *Criminal Code Act 1995* (Criminal Code) provides that 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. Having the fault element of recklessness apply to the physical circumstance in which conduct occurs encourages a person contemplating making a disclosure to turn their mind to the nature of the information they are intending to disclose. A person would always need to keep in mind that disclosing information about an undercover operation without authority—whether or not it is related to a special intelligence operation—may have the potential to jeopardise an ongoing investigation and moreover, may threaten life. The actions of a person to manage risk are directly relevant to an assessment of whether a person's actions were justifiable in the circumstances. The offences would not apply to a person who disclosed information (for example in relation to the conduct of a terrorist attack) entirely unaware that it could relate to a special intelligence operation, since there would be no evidence of advertence to a risk of any kind.

Knowledge under section 5.3 of the Criminal Code, in comparison to recklessness, provides that a person has knowledge of a circumstance or a result if he or she is aware that it exists or will exist in the ordinary course of events. The granting of special intelligence operation authorisations and their use as an investigative tool by ASIO is not a matter for public dissemination because to publicise their deployment would nullify their usefulness as an investigation technique. As such it would be unduly onerous to prove that a person was aware that the information disclosed related to a special intelligence operation in the ordinary course of events (as opposed to relating, for example, to some other type of covert investigation). If the fault element of knowledge is applied,

it will enable the unauthorised disclosure of information relating to a special intelligence operation, which was prejudicial to the operation and the safety of its participants, even where the person was aware there was a substantial risk the information related to a special intelligence operation.

As special intelligence operations are expected to be used only in the most highly sensitive circumstances, the Parliamentary Joint Committee on Intelligence and Security (PJCIS) accepted the need for specific offence provisions to confer a higher level of protection for information than for other operational matters. The PJCIS considered 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. As mentioned earlier, unauthorised discourse of information relating to a special intelligence operation can also prejudice the conduct of other investigations and compromise the effectiveness of ASIO's capabilities and methods employed in the performance of its statutory functions both directly and also indirectly through mosaic effect. The harm arising from an unauthorised disclosure of information relating to a special intelligence operation occurs whether or not the discloser conclusively knows of the existence of an operation.

Does ASIO consider that the offence in subsection 35P(1) could potentially apply to an ASIO officer who provides information to a journalist in these circumstances? Can ASIO provide any general comment on the way in which paragraphs 35P(3)(a) or (d) may potentially operate in relation to the activities of its media liaison officers?

It is ASIO's policy that media liaison officers do not provide comment in relation to individuals, investigations or operations, including in relation to special intelligence operations. In any event, subsection 35P(1) would not apply to an ASIO staff member who provides information to a journalist as long as the ASIO staff member, in this case a media liaison officer, is communicating information in connection with the performance of their functions as the 35P(3)(a) and (d) exceptions would apply.

To communicate ASIO information, a person (including an ASIO employee or ASIO affiliate) must be authorised or approved by the Director-General pursuant to section 18 of the ASIO Act. ASIO media liaison officers are authorised by name in writing by the Director-General to communicate information to journalists and media outlets while performing their duties as a media liaison officer and therefore the exceptions in s35P(3)(a) and (d) will apply. Where information is not communicated in accordance with section 18, offences in addition to section 35P may also apply to that communication. For example subsection 18(2) makes it an offence to communicate ASIO information otherwise than in the course of duties and with the authorisation or approval of the Director-General.

Does ASIO 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?

The inclusion of the note referring to the definition of recklessness in section 5.6 of the Criminal Code for paragraphs 35P(1)(b) and 35P(2)(b), and the omission of the same note for paragraph 35P(2)(c) is not in any way intended to displace or vary the application of the default fault element of recklessness under section 5.6(2) of the Criminal Code.

The note for paragraphs 35P(1)(b) and 35P(2)(b) was specifically included to reassure the PJCIS and to confirm that the correct test to be applied for these offences was the Criminal Code test for recklessness. This approach is legally consistent with the use of notes in Commonwealth legislation, where it is aimed at aiding interpretation and does not affect the ordinary application of the Criminal Code to other offence provisions or parts of offence provisions.