August 2020

Minister's Guidelines

in relation to the performance by the Australian Security Intelligence Organisation of its functions and the exercise of its powers.

FOREWORD

The anticipatory nature of the work of the Australian Security Intelligence Organisation (**ASIO**) is critical to the protection of the nation and its interests from threats to security. ASIO achieves this by performing its statutory functions, including through intelligence collection, analysis and assessment, and by providing advice to government, business and partners.

In performing this role, ASIO must pursue intelligence that enables it to anticipate adverse security events, and cooperate with and assist other agencies and authorities to reduce the potential harm to our national interest. It must conduct investigations into potential and actual security threats, communicate intelligence that enables the powers and capabilities of ASIO and other agencies to be deployed to prevent security incidents, and give security advice that informs government decision-making to manage risks. It must also seek the best approaches to identify and evaluate security threats and emergent sources of harm.

ASIO's role is a complex one that requires a close understanding of evolving risks from disparate sources. Those intending to harm national security frequently seek to conceal their activities. Espionage plots can span decades and have the resources of nation states aimed at obscuring them. Terrorist attack planning can evolve rapidly with little or no forewarning.

As a nation, we expect ASIO to achieve its purpose of contributing to the protection of the nation from security threats and have granted it powers necessary to perform its statutory functions in pursuit of this public good. We expect ASIO to exercise its powers and use its resources judiciously, and that it will only collect and retain information related to or required for the proper performance of its statutory functions. ASIO needs to be empowered to undertake its role – but it must do so within these parameters.

These Guidelines set out the principles ASIO is required to observe in order to meet the public's expectations in performing its functions, including obtaining, correlating and evaluating intelligence relevant to security, and the interpretation of politically motivated violence. In so doing, the Guidelines form a critical component of the accountability framework that provides assurance that ASIO fulfils its vital functions consistent with the values of the community it serves.

The Hon Peter Dutton MP

Minister for Home Affairs

INTRODUCTION

These Guidelines assist ASIO with the performance of its functions in subsection 17(1) of the *Australian Security Intelligence Organisation Act 1979* (**ASIO Act**), by providing guidance to staff in undertaking their duties in accordance with Government and community expectations. These Guidelines also provide guidance to support ASIO in the performance of its functions which relate to politically motivated violence.

Overview

These Guidelines are divided into five parts:

Part 1: Implementing the Guidelines outlines how the Guidelines should be implemented and observed, with the Director-General of Security (**Director-General**) ultimately responsible for the implementation of these Guidelines, and ASIO's compliance with them subject to oversight by the Inspector-General of Intelligence and Security (**IGIS**).

Part 2: Inquiries and investigations guides ASIO on the authorisation and conduct of its inquiries and investigations.

Part 3: Obtaining intelligence relevant to security sets out expectations regarding collection activities undertaken by ASIO in the performance of its functions of obtaining, correlating and evaluating intelligence relevant to security.

Part 4: Treatment of personal information outlines how and when ASIO should handle, retain and destroy personal information. In addition to legislative requirements, ASIO is to have internal policies and practices in place to ensure the appropriate access, management and destruction of records.

Part 5: Politically motivated violence provides guidance to be observed in relation to the performance of ASIO's functions that relate to politically motivated violence.

Key terms applicable to the interpretation of these Guidelines are set out in the **Appendix**.

1. IMPLEMENTING THE GUIDELINES

1.1 These Guidelines are given by the Minister for Home Affairs to the Director-General under subsections 8A(1) and 8A(2) of the ASIO Act and are to be observed by ASIO in the performance of its functions as specified in subsection 17(1) of the ASIO Act, including obtaining, correlating and evaluating intelligence relevant to security.

"**security**" has the meaning given in section 4 of the ASIO Act, being:

a) the protection of, and of the people of, the Commonwealth and the several States and Territories from:

(i) espionage;

(ii) sabotage;

(iii) politically motivated violence;

(iv) promotion of communal violence;

(v) attacks on Australia's defence system; or

(vi) acts of foreign interference;

whether directed from, or committed within, Australia or not; and

aa) the protection of Australia's territorial and border integrity from serious threats; and

b) the carrying out of Australia's responsibilities to any foreign country in relation to a matter mentioned in any of the subparagraphs of paragraph (a) or the matter mentioned in paragraph (aa).

1.2 These Guidelines replace the *Attorney-General's Guidelines in relation to the performance by the Australian Security Intelligence Organisation of its function of obtaining, correlating, evaluating and communicating intelligence relevant to security (including politically motivated violence)* given under subsections 8A(1) and 8A(2) of the ASIO Act in 2007. The Director-General is responsible for ASIO's compliance with these Guidelines.

1.3 The Director-General may require an ASIO employee or ASIO affiliate to be responsible for ensuring that appropriate processes are in place to comply with these Guidelines.

1.4 The Director-General is responsible for deciding ASIO's intelligence collection, analysis and assessment priorities (subject to section 8 of the ASIO Act).

Governing principles

1.5 Under subsection 8(1) of the ASIO Act, the Director-General has legislated responsibilities for the control of ASIO. The Director-General also has legal responsibilities under other legislation, such as the Public Governance, Performance and Accountability Act 2013.

1.6 ASIO shall fulfil its statutory functions under section 17 of the ASIO Act in an impartial manner.

1.7 ASIO works to anticipate and provide timely advice on threats to the security of Australia, the Australian people, and Australian interests, whether in or outside Australia.

1.8 ASIO's security functions are concerned with threat identification and risk mitigation. These functions are anticipatory in nature. ASIO therefore identifies and investigates known, emerging and potential sources of harm in order to understand and, working with others, minimise the gravity of threats posed and the likelihood of their occurrence.

1.9 ASIO implements measures or arrangements, as far as is reasonably possible, to ensure that the information it relies upon is reliable and accurate.

1.10 Section 17A of the ASIO Act provides that the ASIO Act shall not limit the right of persons to engage in lawful advocacy, protest or dissent, and the exercise of that right shall not, by itself, be regarded as prejudicial to security, and the functions of ASIO shall be construed accordingly.

1.11 Section 20 of the ASIO Act provides that the Director-General shall take all reasonable steps to ensure that:

a) ASIO's work is limited to what is necessary for the purposes of the discharge of its functions, and

b) ASIO is kept free from any influences or considerations not relevant to its functions and nothing is done that might lend colour to any suggestion that it is concerned to further or protect the interests of any particular section of the community, or with any matters other than the discharge of its functions.

Oversight by the Inspector-General of Intelligence and Security

1.12 Section 8 of the *Inspector-General of Intelligence and Security Act 1986* provides that the IGIS's functions include inquiring into any matter that relates to ASIO's compliance with these Guidelines. This inquiry may be at the request of the Minister or the Attorney-General, at the IGIS's own motion, or in response to a complaint.

1.13 To facilitate the oversight role of the IGIS, the Director-General will ensure that:

a) the IGIS and authorised IGIS staff have effective access to all information held by ASIO

b) ASIO retains information required to demonstrate its propriety, compliance with applicable laws of the Commonwealth and of the States and Territories, and directions given to ASIO by the responsible Minister, and

c) copies of the policies made for the purposes of paragraphs 2.15 and 4.3 of these Guidelines are provided to the IGIS as soon as practicable after they are made or amended.

Review

1.14 The operation and continued suitability of these Guidelines will be reviewed in consultation with relevant stakeholders and ministers as appropriate, on a periodic basis as follows:

a) the first review will commence within 18 months, and be completed within three years after commencement of these Guidelines, and

b) by every third anniversary of the Guidelines thereafter, a further review must be completed.

1.15 The Attorney-General will be notified of the outcome of any Review conducted under paragraph 1.14.

2. INQUIRIES AND INVESTIGATIONS

2.1 ASIO inquiries[1] and investigations[2] should be concerned with performing ASIO's security functions by obtaining, correlating and evaluating intelligence about individuals, groups or other entities – including their intentions and capabilities – in order to identify and investigate known and emerging threats. ASIO is required to:

a) undertake inquiries to identify persons, groups or other entities (subjects), and determine whether their activities are likely relevant to security and merit investigation subject to paragraphs 2.4 and 2.5

b) investigate subjects' activities in order to understand and minimise the gravity of threats posed and the likelihood of their occurrence

c) develop and maintain a broad understanding of the security environment, and

d) analyse and assess information obtained, and to provide intelligence and advice to relevant authorities.

Authorisation of investigations

2.2 The initiation and continuation of investigations will be authorised only by:

a) the Director-General, or

b) an ASIO employee or ASIO affiliate at or above Executive Level 2 (or equivalent) authorised by the Director-General for that purpose, or

c) in specific, limited circumstances where a person listed in subparagraphs (a) or (b) is ordinarily unavailable to authorise the initiation or continuation of particular investigations, an ASIO employee or ASIO affiliate at Executive Level 1 (or equivalent) may be authorised by the Director-General for that purpose.

Conducting investigations

2.3 Decisions to initiate investigations will be based on a consideration of the extent to which the activities of a subject will, or are likely to, cause harm or damage,

---

[1] As defined at Appendix 1: For the purposes of these Guidelines, ***inquiry*** means action taken to obtain information for the purpose of identifying a subject and/or determining whether the activities of a subject are likely relevant to security. This can be part of an investigation.

[2] As defined at Appendix 1: For the purposes of these Guidelines, ***investigation*** means action to investigate a subject's activities that are likely relevant to security as authorised under paragraph 2.2, having had regard to the consideration set out in paragraphs 2.3 and 2.4.

ASIO's overall priorities, and the availability of appropriate resources. ASIO is not required to investigate every matter that is likely relevant to security.

2.4 In deciding whether to conduct an investigation, and the investigative methods to be used, ASIO will consider:

a) what is already known about a subject's activities, associations and beliefs, and the extent to which those activities, associations and beliefs are, or are likely to be, prejudicial to security

b) the immediacy and severity of any threat to security

c) the reliability of the sources of the relevant information, and

d) subject to paragraph 3.4 of these Guidelines, the investigative techniques that are likely to be most effective and efficient.

Review of inquiries and investigations

2.5 Ongoing investigations are to be reviewed no less than annually.

2.6 Records of inquiries and investigations will be handled in accordance with Part 4 of these Guidelines.

Advice to the Minister

2.7 The Director-General will keep the Minister advised, in general terms, of ASIO's investigations and priorities through:

a) regular briefings to the Minister on ASIO's investigations, significant developments in relation to important subjects, and the emergence of significant new subjects, and

b) other means as necessary.

Warrants

2.8 All ASIO Act warrants are issued by the Attorney-General, unless otherwise provided in Division 3 of Part III of the ASIO Act. With respect to ASIO Act warrants, the Director-General must, within a reasonable period, report to the Attorney-General on:

a) the extent to which the action taken under every warrant has assisted ASIO in carrying out its functions

b) other matters set out in section 34 of the ASIO Act – for example, if an order was made under subsection 34AAA(2) in relation to a warrant, the

report must also include details of the extent to which compliance with the order has assisted ASIO in carrying out its functions

c) any breaches by ASIO of any conditions or restrictions specified in a warrant, and

d) any action taken which would have required a warrant where one had not been obtained.

2.9 All *Telecommunications (Interception and Access) Act 1979* (**TIA Act**) warrants authorising ASIO to intercept communications and access stored communications are issued by the Attorney-General. With respect to such warrants, the Director-General must, within three months after the expiration or revocation, whichever first occurs, of the warrant, report to the Attorney General on:

a) the extent to which the interception of communications and access to stored communications under the warrant has assisted ASIO in carrying out its functions and the other matters set out in section 17 of the TIA Act

b) any breaches by ASIO of any conditions or restrictions specified in a warrant, and

c) any action taken which would have required a warrant where one had not been obtained.

Special intelligence operations

2.10 Special intelligence operations are authorised by the Attorney-General under section 35C of the ASIO Act. Where a special intelligence operation has been authorised, the Director-General must give a written report to the Attorney-General and the IGIS:

a) on the extent to which each special intelligence operation has assisted ASIO in the performance of one or more special intelligence functions (subsection 35Q(2) of the ASIO Act), including a description of the nature of the special intelligence conduct engaged in during the course of the special intelligence operation

b) reporting on whether the conduct of a participant in a special intelligence operation caused the death of, or injury to, any person; or involved the commission of a sexual offence against any person; or resulted in loss of, or damage to, property (subsection 35Q(2A) of the ASIO Act)

c) any breaches of any conditions to which the conduct of a special intelligence operation is subject, and

d) details of any conduct reasonably believed to be unlawful engaged in by a participant in relation to a special intelligence operation that was not authorised.

Leader of the Opposition to be kept informed on security matters

2.11 Section 21 of the ASIO Act requires the Director-General to consult regularly with the Leader of the Opposition in the House of Representatives for the purpose of keeping him or her informed on matters relating to security.

Security assessments

2.12 The furnishing by ASIO of security assessments to a Commonwealth agency or State or authority of a State is governed by Part IV of the ASIO Act. Where it is necessary to obtain new information relevant to a security assessment, including an assessment which is yet to be made, such inquiries or investigations will be conducted in accordance with these Guidelines.

Use of force against the person under warrant

2.13 The Director-General will take all reasonable steps to ensure that persons, including ASIO employees, who are authorised to use force against a person under an ASIO warrant are appropriately trained.

2.14 The Director-General is entitled to presume that the following categories of persons are appropriately trained:

a) Sworn members of the Australian Federal Police, or of a police force of a State or Territory.

b) Other Commonwealth, State and Territory officials, who would ordinarily be expected to use force as part of their duties.

2.15 ASIO will maintain policies in respect of paragraphs 2.13 and 2.14.

2.16 Section 2.13 does not limit the inherent right of an ASIO employee or ASIO affiliate to self-defence.

3. OBTAINING INTELLIGENCE RELEVANT TO SECURITY

3.1 These Guidelines apply to all collection activities undertaken by ASIO in the performance of its function of obtaining, correlating and evaluating intelligence relevant to security in accordance with paragraph 17(1)(a) of the ASIO Act. This includes collection of information under warrant and authorisations for access to telecommunications data made under the TIA Act.

3.2 In performing its functions, subject to Part 4 of these Guidelines, ASIO may:

a) collect, maintain, analyse and assess information relevant to security

b) collect and maintain a comprehensive body of reference data to contextualise intelligence derived from inquiries and investigations, and

c) maintain a broad database against which information obtained in relation to a specific inquiry or investigation can be checked and assessed.

3.3 The Director-General will establish processes to ensure that all of ASIO's requests for information from external agencies are authorised at an appropriate level.

Proportionality of ASIO Activities

3.4 Information is to be collected by ASIO in a lawful, timely and efficient way, and in accordance with the following principles:

a) any means used for obtaining and analysing information must be proportionate to the gravity of the threat posed and the likelihood of its occurrence, including by having regard to potential impacts on third parties,

b) inquiries and investigations into individuals and groups should be undertaken:

i. using as little intrusion into the privacy of affected individuals as is reasonably required, consistent with the performance of ASIO's functions, and

ii. with due regard for the cultural values, mores and sensitivities of individuals of particular cultural or racial backgrounds, consistent with the national interest,

c) the intrusiveness of techniques or methods for collecting information are to be considered in determining approval levels for their use. More intrusive techniques or methods should generally require a higher level ASIO

employee or ASIO affiliate to approve their use, consistent with paragraph 2.2.

d) where possible, the least intrusive techniques for collecting information should be used before more intrusive techniques

e) where a threat is assessed as likely to develop quickly, a greater degree of intrusion may be justified

f) the likely impact on any person of using the technique is to be considered

g) whether the person has consented to the use of the technique is to be considered, and

h) the sensitivity and volume of information being collected should be considered.

Note: Section 4.3 of these Guidelines provides that ASIO must maintain policies around its access to and retention of personal information.

3.5 Where the Director-General, or relevant delegate, is considering requesting assistance from a person or body in accordance with section 21A of the *ASIO Act* or in accordance with Part 15 of the *Telecommunications Act 1997* in circumstances where a civil or criminal immunity could arise, proportionality must be considered. In determining proportionality, the Director-General should consider the seriousness of any offence or conduct to which the immunity may apply and the impact on innocent parties.

3.6 ASIO will maintain policies in respect of paragraph 3.5.

Accuracy of information

3.7 ASIO will take all reasonable steps to ensure that personal information used or disclosed by ASIO is relevant, accurate, and not misleading.

Collecting intelligence relevant to security

3.8 Intelligence collected may include, but is not limited to, information relating to:

a) the identity and relevant activities of individuals, groups or other entities of interest, including persons associated with a group or person of interest and other persons likely to be knowingly concerned in furtherance of its plans or activities, and

b) the finances, the geographic dimensions, and the past, present and prospective activities of individuals, groups or other entities of interest.

4. TREATMENT OF PERSONAL INFORMATION

4.1 ASIO will only collect, use, handle, retain or disclose personal information for purposes related to the performance of its functions or exercise of its powers, or where otherwise authorised, or required, by law.

4.2 The Director-General will take all reasonable steps to ensure that ASIO's collection, retention, use, handling, and disclosure of personal information is limited to what is reasonably necessary to perform its functions. This includes having reasonable controls to prevent the collection and processing of information in breach of a warrant or statutory authority, and procedures for appropriate remediation and reporting should this occur.

4.3 ASIO will maintain policies about its access to, and retention of, personal information.

a) These policies must provide clear guidance on:

i. the type of personal information ASIO collects and retains

ii. how ASIO should collect, hold, retain, protect and access personal information

iii. the circumstances and associated requirements around the de-identification of personal information

iv. the purposes for which ASIO may collect, hold, retain, use, access and disclose personal information

v. the disclosure of information overseas, including its effect on individual privacy interests

vi. processes for periodic review of its holdings, including personal information, to determine whether retention is reasonable, and

vii. setting, reviewing and undertaking disposal actions in accordance with the ASIO Records Authority and any other Commonwealth recordkeeping directives or legislative requirements.

b) These policies must require ASIO to:

i. ensure that it retains personal information only:

a. when it is relevant to the proper performance of its functions or exercise of its powers, or

b. where otherwise authorised, or required, by law

ii. ensure only ASIO employees and ASIO affiliates who require access to data and information, which may include reference data, for the proper performance of their duties are authorised to do so

iii. maintain internal audit mechanisms which provide assurance that ASIO employees and ASIO affiliates who are authorised to access data and information, which may include reference data, do so only for the proper performance of their duties, and

iv. report to the IGIS any collection of, or access to, data, which may include reference data, which are inconsistent with, or in contravention of legislation.

Note: This section of the Guidelines does not apply to ASIO's corporate business information or data.

Note: Under the *Inspector-General of Intelligence and Security Act 1986*, the IGIS may review access by ASIO employees and ASIO affiliates to data and information.

Note: Guidelines on the destruction of records are at paragraph 4.11.

Security and access to personal information holdings

4.4 Where ASIO retains personal information, the Director-General will ensure that:

a) the information is protected, by such safeguards as are reasonable in the circumstances, against:

i. loss

ii. unauthorised access, use, modification or disclosure, and

iii. other misuse or interference,

b) access is limited to those ASIO employees or ASIO affiliates who require it for the performance of their roles and functions, consistent with the ASIO Act, ASIO Code of Conduct, and ASIO's security and information management policies, and

c) access is available to the IGIS and authorised IGIS staff, in the performance of their functions.

Compliance with Commonwealth recordkeeping requirements

4.5 ASIO will manage its records in accordance with the *Archives Act 1983* (the Archives Act) and any additional recordkeeping directives issued by the National Archives of Australia, including the ASIO Records Authority.[3]

4.6 Consistent with legislative requirements, the ASIO Records Authority permits ASIO to dispose[4] of certain classes of records under the Archives Act after the relevant minimum retention period has expired and where they are no longer needed for agency business. It also identifies the classes of records required to be retained as part of the archival resources of the Commonwealth. ASIO may refer to retained records where there is an ongoing need to do so for ASIO's performance of its functions.

4.7 Minimum retention periods set by the ASIO Records Authority are approved by the National Archives of Australia and are based on an assessment of business needs, broader ASIO legal and accountability requirements, and community expectations. These minimum retention periods are applied to files on creation and reviewed as appropriate.

4.8 The Director-General will ensure that appropriate internal policies and procedures are in place to inform the setting and reviewing of disposal classes applied to records under the ASIO Records Authority.

4.9 Subject to paragraph 4.13, appropriate records will be kept of all external requests made by ASIO for access to personal information and all personal information received in response to such requests.

4.10 Subject to paragraph 4.13, appropriate records will be kept of all disclosures by ASIO of personal information for purposes relevant to security or as otherwise authorised.

Disposal of records

4.11 ASIO must take reasonable steps to destroy or otherwise dispose of personal information where that personal information is:

a) not required by ASIO for the performance of its functions or exercise of its powers, and

---

[3] The ASIO Records Authority is publicly available from the National Archives of Australia (www.naa.gov.au).

[4] Under the Archives Act 1983 disposal of Australian Government information means either its destruction, the transfer of its custody or ownership, or damage or alteration (www.naa.gov.au/information-management/disposing-information/information-disposal).

b) not required to demonstrate propriety, compliance by ASIO with laws of the Commonwealth and of the States and Territories, or directions and guidelines given to ASIO by the Minister.

4.12 Disposal may include the de-identification[5] of personal information. ASIO may retain information that has been de-identified, and which is therefore no longer personal information, for the performance of its functions or exercise of its powers consistent with legislative requirements.

4.13 Subject to paragraph 4.11, the Director-General will ensure that in accordance with applicable legislative requirements:

a) after the minimum retention period for a record (including a record containing personal information) has expired, and

b) where ASIO's review processes have determined the record is no longer needed for the proper performance of ASIO's functions,

the relevant record will be destroyed in accordance with the ASIO Records Authority.

4.14 The Director-General will ensure all ASIO employees and ASIO affiliates are aware of, and adhere to, internal policies and procedures for the disposal of information.

4.15 ASIO will comply with obligations under the ASIO Act, the ASIO Records Authority and any other applicable Commonwealth recordkeeping directives or legislative requirements which requires the destruction or disposal of records or copies of records.

[5] As defined at Appendix 1: ***de-identified*** means the removal of direct identifiers and one or both of the removal or alteration of other information that could potentially be used to re-identify an individual, and/or the use of controls and safeguards in the data access environment to prevent re-identification. Note: this is consistent with guidance from the Office of the Australian Information Commissioner: https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-and-the-privacy-act/.

5. POLITICALLY MOTIVATED VIOLENCE

5.1 This part of the Guidelines is issued in accordance with subsection 8A(2) of the ASIO Act and must be observed by ASIO in performing its functions that relate to politically motivated violence.

Legislative definitions

5.2 Key provisions of the ASIO Act relating to politically motivated violence are:

a) the definition of politically motivated violence in section 4, and

b) section 17A, which provides that the ASIO Act is not concerned with lawful advocacy, protest, or dissent (see paragraph 1.10 above).

5.3 As at the date of these Guidelines, politically motivated violence is defined in the ASIO Act as:

a) acts or threats of violence or unlawful harm that are intended or likely to achieve a political objective, whether in Australia or elsewhere, including acts or threats carried on for the purpose of influencing the policy or acts of a government, whether in Australia or elsewhere; or

b) acts that:

i. involve violence or are intended or are likely to involve or lead to violence (whether by the persons who carry on those acts or by other persons), and

ii. are directed to overthrowing or destroying, or assisting in the overthrow or destruction of, the government or the constitutional system of government of the Commonwealth or of a State or Territory; or

ba) acts that are terrorism offences;[6] or

c) acts that are offences punishable under Division 119 of the *Criminal Code Act 1995*, the *Crimes (Hostages) Act 1989* or Division 1 of Part 2, or Part 3, of the *Crimes (Ships and Fixed Platforms) Act 1992* or under Division 1 or 4 of Part 2 of the *Crimes (Aviation) Act 1991*; or

[6] Section 4 of the ASIO Act defines terrorism offence as: (a) an offence against Subdivision A of Division 72 of the Criminal Code; or (b) an offence against Part 5.3 of the Criminal Code. Note: A person can commit a terrorism offence against Part 5.3 of the Criminal Code even if no terrorist act (as defined in that Part) occurs.

d) acts that:

i. are offences punishable under the *Crimes (Internationally Protected Persons) Act 1976,* or

ii. threaten or endanger any person or class of persons specified by the Minister for the purposes of this subparagraph by notice in writing given to the Director-General.

Interpreting politically motivated violence

Subparagraph (a) of the definition of politically motivated violence

5.4 The activity comprehended by subparagraph (a) of the definition of politically motivated violence includes terrorism, and violent protest that has a political objective, and acts of hostage-taking within the meaning of the section 7 of the *Crimes (Hostages) Act 1989.* In performing its functions in relation to subparagraph (a) of the definition of politically motivated violence, ASIO should give priority to persons or groups likely to be involved in:

a) acts or threats of serious violence or unlawful harm designed to create fear or to incite or provoke violent reaction, or

b) the use of tactics that can reasonably be assessed as likely to result in violence,

in order to achieve a political objective.

5.5 The above considerations apply whether the object of the violent act or threat is the government of the Commonwealth, a State or Territory, the government of a foreign country with which Australia has responsibilities in relation to security matters, or the people of Australia or Australian interests within Australia and overseas. Where acts or threats occur within an Australian State or Territory and appear wholly designed to influence the policy or acts of the State or Territory government, ASIO is to inform the Minister of any decision taken to investigate such acts or threats.

Subparagraph (b) of the definition of politically motivated violence

5.6 In performing its functions in relation to subparagraph (b) of the definition of politically motivated violence, ASIO is to investigate whether a person or a group actively holds to, advocates or encourages a doctrine, or pursues political objectives in which advocacy of the use of violence is accepted for the purpose of overthrowing, destroying or assisting in the overthrow or destruction of a government or the constitutional system of government of the Commonwealth, or a State or Territory.

5.7 Whether it is probable that the activity will succeed in its purpose and whether the intent is for imminent or future activity are matters which ASIO should take into account in setting its priorities. However, these considerations of probability of success or imminence of violence are not factors which of themselves determine whether the act is politically motivated violence.

5.8 A person or group need not intend to initiate violence in the process of overthrowing constitutional government for their activities to be assessed as politically motivated violence under subparagraph (b). It is sufficient if the activities could lead to violence. All that is required is that there is a reasonable likelihood that the activity will produce violence from others.

5.9 Advocacy of violence may come within subparagraph (b) of the definition of politically motivated violence even though it is not itself unlawful, or the advocacy is not public. Of their very nature, preparations directed at the overthrow of government are likely to be clandestine and their early manifestations are deceptive.

5.10 If apparently non-violent activities directed at destabilising or undermining constitutional government are associated with what purports to be no more than contemplation of the prospect of the violent overthrow of government, ASIO may investigate those activities to the extent necessary to establish (with some confidence) whether the activities involve a real risk or danger that violence will flow from those activities.

Subparagraphs (ba) and (c) of the definition of politically motivated violence

5.11 Subparagraphs (ba) and (c) of the definition of politically motivated violence refer to activities that are criminal offences. Any activity which may constitute a criminal offence under the legislation specified is an act of politically motivated violence.

Subparagraph (d) of the definition of politically motivated violence

5.12 Subparagraph (d) of the definition of politically motivated violence refers to attacks on the persons, official premises and private accommodation of certain defined persons and provides for the Minister to add to those defined persons by specifying by notice in writing to the Director-General.

5.13 The categories of persons defined by subparagraph (d) of the definition of politically motivated violence include internationally protected persons as defined by the *Crimes (Internationally Protected Persons) Act 1976*. Any activity which may constitute a criminal offence under this legislation is an act of politically motivated violence.

5.14 Subparagraph (d)(ii) also provides for the Minister to add other persons by notice in writing to the Director-General. Those persons might vary from time to time, and could include:

a) Ministers of the Commonwealth Government

b) the Leader of the Opposition in the Commonwealth Parliament

c) Members of the Commonwealth Parliament when travelling as a Parliamentary delegation, and

d) the Premiers and Chief Ministers of the States and Territories.

5.15 Section 5A of the ASIO Act requires the Minister to give the IGIS a copy of a notice given to the Director-General for the purposes of subparagraph (d)(ii).

Investigations into demonstrations and other forms of protest

5.16 Further to Part 2 of these Guidelines, the following guidance relates specifically to ASIO's investigation of demonstrations and other forms of protest.

5.17 ASIO is not to undertake investigations where the only basis for the investigation is the exercise of a person's right of lawful advocacy, protest or dissent (section 17A of the ASIO Act).

5.18 ASIO is not to investigate demonstrations or other protest activity unless:

a) there is a risk of pre-meditated use of violence against persons or property for the purposes of achieving a political objective, or pre-meditated use of tactics that can be reasonably assessed as likely to result in violence, or

b) it suspects there is a link between the demonstration or other protest activity and conduct coming otherwise within the definition of security.

5.19 An exception to the above is demonstrations or other protest activity against internationally protected persons or other persons specified by the Minister under subparagraph (d)(ii) of the definition of politically motivated violence.

5.20 Minor acts of violence, such as jostling or defacing or damaging property, are properly matters for investigation by a police force, as are incidental acts of violence or property damage which occur in the course of a demonstration. Where, however, such acts are or are intended to be part of a pattern, and where there is reason to believe that the acts are intended to influence the policy or acts of a government, ASIO may investigate to determine whether there is a potential for the violence to escalate or become more strongly directed at a person or group associated with the policy or acts at issue.

Assessment of politically motivated violence

5.21 ASIO's threat assessment function is an integral part of national arrangements for the protection of high office holders, internationally protected persons, sites of national significance and critical infrastructure. ASIO may prepare threat assessments in relation to any demonstration or protest activity on the basis of information it already has or which is passed to it by other agencies, for the purpose of advising authorities responsible for law enforcement and the protection of designated persons.

5.22 ASIO is not required to provide an assessment for every event, place, person or instance, that is actually or potentially at threat from politically motivated violence. The Director-General shall consider the potential seriousness of any matter or information, ASIO's priorities, and the availability of appropriate resources.

APPENDIX 1: INTERPRETATION

In these Guidelines:

"**ASIO affiliate**" has the meaning given in section 4 of the ASIO Act, being:

> a person performing functions or services for the Organisation in accordance with a contract, agreement or other arrangement, and includes a person engaged under section 85 and a person performing services under an agreement under section 87, but does not include the Director-General or an ASIO employee.

"**de-identified**" means the removal of direct identifiers and one or both of the removal or alteration of other information that could potentially be used to re-identify an individual, and/or the use of controls and safeguards in the data access environment to prevent re-identification.

"**intelligence relevant to security**" includes information that may assist in determining whether:

a) there is a connection or possible connection between a subject and activities relevant to security, irrespective of when such activities have occurred or may occur

b) the activities of a subject are not relevant to security, or

c) a person, group or entity other than a subject has a connection or possible connection to activities relevant to security.

"**inquiry**" means action taken to obtain information for the purpose of identifying a subject and/or determining whether the activities of a subject are likely relevant to security. This can be as part of an investigation.

"**investigation**" means action to investigate a subject's activities that are likely relevant to security as authorised under paragraph 2.2, having had regard to the considerations set out in paragraphs 2.3 and 2.4.

"**personal information**" means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

a) whether the information or opinion is true or not, and

b) whether the information or opinion is recorded in a material form or not.

"**subject**" means, unless the context otherwise requires, a person, group or other entity.