Australian Government
Department of Home Affairs

Submission to Review of the National Security Legislation Amendment (Comprehensive Review and Other Measures No. 3) Bill 2023

Parliamentary Joint Committee on Intelligence and Security

2 February 2024

Table of Contents

List of Abbreviations

Term	Meaning
AAT	Administrative Appeals Tribunal
AAT Act	*Administrative Appeals Tribunal Act 1975*
Archives Act	*Archives Act 1983*
ASD	Australian Signals Directorate
ASIO	Australian Security Intelligence Organisation
ASIO Act	*Australian Security Intelligence Organisation Act 1979*
ASIS	Australian Secret Intelligence Service
The Bill	National Security Legislation Amendment (Comprehensive Review and Other Measures No. 3) Bill 2023
Comprehensive Review	Comprehensive Review of the Legal Framework of the National Intelligence Community
The Department	The Department of Home Affairs
IGIS	Inspector-General of Intelligence and Security
IS Act	*Intelligence Services Act 2001*
NIC	National Intelligence Community
PAA	Prescribed administrative action
SA	Security assessment
SCD	Security clearance decision
SCSA	Security clearance suitability assessment
TIA Act	*Telecommunications (Interception and Access) Act 1979*

Introduction

1. The Department of Home Affairs (the Department) welcomes the opportunity to provide a submission to the Parliamentary Joint Committee on Intelligence and Security's review of the National Security Legislation Amendment (Comprehensive Review and Other Measures No. 3) Bill 2023 (the Bill).

2. The Department notes the Bill will strengthen the legal framework of the National Intelligence Community (NIC) by implementing 12 recommendations of the Comprehensive Review of the Legal Framework of the National Intelligence Community (Comprehensive Review) led by Mr Dennis Richardson AC. A small number of additional reforms, identified as necessary in consultation with NIC agencies, are also introduced in the Bill.

3. The Department supports targeted reforms to legislation governing Australia's intelligence agencies to address critical challenges they face and to ensure that the legal framework of the NIC keeps pace with an increasingly complex operational environment. Our laws must continue to keep pace with the evolving operational environment and changes in technology to ensure intelligence agencies have the powers — and capabilities — they need to keep Australians safe against a range of existing and emerging threats. Equally, we must continue to ensure appropriate oversight of their work is maintained.

4. The Department also notes that alongside the measures in the Bill, Australia's intelligence agencies remain subject to a range of strict safeguards, independent oversight, and transparency and accountability mechanisms under Australian law.

Background

5. On 4 December 2020, the then Attorney-General released the unclassified report of the Comprehensive Review and the Government's response. The Comprehensive Review was the most significant review of intelligence legislation since the Royal Commissions of the 1970s and 1980s led by Justice Robert Hope AC CMG QC (the Hope Royal Commissions). The Comprehensive Review closely examined the effectiveness of the legislative framework governing the NIC and found that, on the whole, the legal framework governing Australia's intelligence agencies is based on sound principles and has been well-maintained. However, the Comprehensive Review did recognise the need for targeted reforms to the framework and made key recommendations to undertake wholesale reform of Australia's electronic surveillance laws. The Comprehensive Review noted that these targeted reforms are necessary to ensure our intelligence agencies can undertake their functions effectively and keep Australians safe.

6. The Bill is the latest in a series of bills that have implemented recommendations from the Comprehensive Review. These include the National Security Legislation Amendment (Comprehensive Review and Other Measures No. 1) Bill 2021 which implemented 13 recommendations of the Comprehensive review and commenced on 1 April 2022, and the National Security Legislation Amendment (Comprehensive Review and Other Measures No. 2) Bill 2023 which implemented 10 recommendations of the Comprehensive review and commenced on 12 August 2023.

Overview of the Bill

7. The Bill is divided into four schedules:
    a. Schedule 1: ASIO security assessments;
    b. Schedule 2: Protecting identities and information;
    c. Schedule 3: Authorisations for intelligence activities; and
    d. Schedule 4: Security vetting and security clearance related activities.
8. Schedule 1 of the Bill would:
    a. extend the definition of prescribed administrative action (PAA) to decisions relating to parole, firearms licences and security guard licences and enable new categories of PAA to be prescribed by the regulations;
    b. clarify the application of the definitions in section 35 throughout Part IV;
    c. enable ASIO to communicate information to a Commonwealth agency, a state or an authority of a state under subsection 18(3) or 19A(4), for the purposes of PAA that is a decision relating to firearms licences and security guard licences;
    d. clarify that a decision under the *Foreign Acquisitions and Takeovers Act 1975* does not constitute PAA;
    e. enable ASIO to make a preliminary communication to Commonwealth agencies, states or authorities of a state on an urgent and temporary basis, where the information could be used for the purposes of certain PAA; and
    f. require ASIO to notify the Inspector-General of Intelligence and Security (IGIS) where certain security assessments are not furnished within 12 months.
9. Schedule 2 of the Bill would:
    a. improve and enable cover employment arrangements and associated protections for current and former ASIO employees, ASIO affiliates and staff members of the ASIS, and ASD;
    b. consolidate secrecy offences relating to ASIS, ASD, the Australian Geospatial Intelligence Organisation (AGO) and the Defence Intelligence Organisation (DIO);
    c. make exempt under the Archives Act records that identify ASIO or ASIS employees, affiliates and agents; and
    d. update and modernise the publication offence in the ASIO Act and introduce a new disclosure offence.
10. Schedule 3 of the Bill would:
    a. enable the Minister for Foreign Affairs and the Minister for Defence to authorise certain activities before the Attorney-General gives their agreement to the authorisation. The authorisation will not take effect until the Attorney-General's agreement has been obtained;
    b. clarify that the Minister for Foreign Affairs and the Minister for Defence can authorise ASIS, ASD and AGO to undertake activities relating to an Australian person who is likely to be involved in activities that present a risk to their own safety, or are themselves involved in activities relating to a contravention of a UN sanction enforcement law;
    c. remove the ability for a junior Minister to exercise a power under the ASIO Act or TIA Act; and
    d. permit only the Director-General of Security to apply for an authority to conduct a special intelligence operation on behalf of ASIO.

11. Schedule 4 of the Bill would:
    a. clarify the application of the definitions in section 82A throughout the ASIO Act;
    b. enable efficiencies in the processing of non-prejudicial security clearance suitability assessments by permitting the Director-General of Security to delegate their power or function to furnish non-prejudicial security clearance suitability assessments; and
    c. require ASIO to notify the Inspector-General of Intelligence and Security where certain security clearance decisions (SCD) and security clearance suitability assessments (SCSA) are not made or furnished within 12 months.
12. The Bill also makes consequential amendments to the:
    a. *Administrative Appeals Tribunal Act 1975* (AAT Act),
    b. *Archives Act 1983* (Archives Act),
    c. *Australian Crime Commission Act 2002,*
    d. *Australian Security Intelligence Organisation Act 1979* (ASIO Act),
    e. *Business Names Registration Act 2011,*
    f. *Commonwealth Registers Act 2022,*
    g. *Corporations Act 2001,*
    h. *Criminal Code Act 1995,*
    i. *Freedom of Information Act 1982,*
    j. *Intelligence Services Act 2001* (IS Act),
    k. *National Consumer Credit Protection Act 2009,*
    l. *Privacy Act 1988,*
    m. *Telecommunications (Interception and Access) Act 1979* (TIA Act),

Schedule 1 – ASIO security assessments

1.1. Schedule 1, Part 1 – Prescribed administrative action

1.1.1. Division 1 – Decisions in relation to parole, firearm licences and security guard licences

1. Amendments by this division would implement recommendation 193 of the Comprehensive Review by altering the application of Part IV of the ASIO Act in respect of certain decisions. Part IV sets out the manner in which ASIO may provide advice to Commonwealth agencies, states, and authorities of a state. It also provides a mechanism for review of adverse or qualified security assessments in the Administrative Appeals Tribunal (AAT).

2. The proposed amendments by this division would provide that the exercise of power or the performance of functions in relation to a decision relating to parole, firearms and security guard licences is considered PAA. These amendments will not change ASIO's ability to provide advice to states and territories or their authorities about an individual's suitability to hold firearms or security guard licences, and to provide advice in relation to parole decisions. The amendments, however, would ensure the individual affected by the decision is to be notified of the advice and allows for review by the AAT. This amendment would also provide for circumstances in which ASIO may communicate information, not amounting to a security assessment, relating to these decisions.

3. The amendment balances ASIO's role in communicating intelligence for purposes relevant to security, with protecting individuals' rights. Specifically, it ensures that individuals affected by prejudicial security assessments in relation to parole, security guard licences and firearms licences are entitled to notice and review rights under Part IV of the ASIO Act.

1.1.2. Division 2 – Regulations to prescribe actions as a Prescribed Administrative Action

4. Amendments by this division would implement recommendation 194 of the Comprehensive Review by providing a mechanism to introduce new classes of PAA, for the purposes of determining whether a recommendation, opinion or advice by ASIO constitutes a security assessment for the purposes of Part IV of the ASIO Act.

5. The Comprehensive Review noted that despite the breadth of the term "PAA", it is clear that it will not capture all circumstances in which ASIO assessments may substantially adversely affect a person. It is possible that further categories of actions will need to be added to the definition in future. Changes to the definition of PAA currently require legislative amendments to alter the definition in section 35 of the ASIO Act. Inserting a regulation-making power will allow for new categories to be added quickly into the definition of PAA, subject to review by the Parliamentary Joint Committee on Intelligence and Security (PJCIS). This will ensure ASIO advice continues to be appropriately subject to notice and review rights as new categories of decisions requiring security advice emerge.

1.2. Schedule 1, Part 2 – Security assessment and preliminary communications

1.2.1. Division 1 – Decisions under the Foreign Acquisitions and Takeovers Act 1975

6. This division would implement recommendation 197 of the Comprehensive Review by amending the application of Part IV of the ASIO Act in respect of certain decisions. Specifically, this division would provide that decisions made under the Foreign Acquisitions and Takeovers Act 1975 or the regulations under that Act are not PAA. As such, a recommendation, opinion or advice by ASIO under that Act or associated regulations would not constitute a security assessment for the purposes of Part IV.

7. The Comprehensive Review noted that in the case of foreign companies it is incongruous that merits review would be available in respect of ASIO security assessments provided to the Foreign Investment Review Board, when the Treasurer's decisions under the Foreign Acquisitions and Takeovers Act 1975, taken on advice from the Board, are exempt from review under the Administrative *Decisions (Judicial Review) Act 1977*.

8. The Department notes that foreign companies seeking to make major investments in Australia have the potential to pose a risk to national security. Normally, these companies are making legitimate investments that can benefit Australian national and local economies. However, some companies have links to the governments of foreign states or are obliged to comply with laws in their home country to share information with state authorities. As foreign companies are not Australian it would be inappropriate to permit access to the notification and review rights in Part IV of the ASIO Act.

1.2.2. Division 2 – Clarification of effect of definitions on certain security assessments

9. This division would insert a reference to section 35 in subsection 36(1), to ensure the defined terms set out in section 35 apply in respect of security assessments to which Part IV does not otherwise apply. Section 35 contains a number of definitions for the purposes of Part IV of the Act. Section 36 sets out certain security assessments to which the notice and review provisions of Part IV does not apply. In addition the chapeau in subsection 36(1) provides an exception for these security assessments so that subsections 37(1), 37(3) and 37(4) (which are in Part IV of the Act) will apply to these security assessments. By inserting a reference to section 35 into subsection 36(1), the amendment clarifies that the definitions in section 35 apply to the security assessments described in section 36 to which Part IV of the Act does not otherwise apply.

1.2.3. Division 3 – Preliminary communications to states

10. This division would implement recommendation 198 of the Comprehensive Review by amending the ASIO Act to enable ASIO to communicate information, whether directly, or indirectly through a Commonwealth agency, to a state or an authority of a state for the purpose of enabling that state or authority to take certain PAA, where it would be necessary as a matter of urgency to take that action.

11. The Comprehensive Review noted that, over time, ASIO has been called on to provide security assessments to state and territory authorities more regularly. However, Part IV of the ASIO Act prohibits ASIO from furnishing otherwise than in the form of a security assessment, information, recommendation, opinion or advice concerning a person, which ASIO knows is intended or likely to be used by a state or authority of the state in considering PAA in relation to that person. The amendment made by Division 3 would enable ASIO to communicate information, whether directly, or indirectly through a Commonwealth agency, to a state or an authority of a state for the purpose of enabling that state or authority to take certain PAA, where it would be necessary, as a matter of urgency to take that action. These provisions are modelled on the existing section 39, which relate to Commonwealth agencies.

12. In addition, the Bill provides that should ASIO provide a preliminary communication, ASIO would be required to furnish a security assessment, to inform the taking of permanent action. It is expected that ASIO would furnish a security assessment as soon as reasonably practicable following a preliminary communication, taking into account the circumstances of each case.

1.2.4. Division 4 – Temporary action by Commonwealth agencies

13. This division would amend the ASIO Act to expand the circumstances in which a Commonwealth agency can take PAA, on the basis of a communication made by ASIO not amounting to a security assessment, where it would be necessary as a matter of urgency to take that action. These provisions are a consequence of the new categories of PAA that would be introduced by Division 1.

1.3. Schedule 1, Part 3 & Schedule 4, Part 2 – Delayed security assessments, security clearance suitability assessments and security clearance decisions

14. Schedule 1, Part 3 of the Bill would respond to recommendation 199 of the Comprehensive Review. It would require ASIO to notify the IGIS where certain security assessments (SA) are not furnished within 12 months, pursuant to Part IV of the ASIO Act.

15. Schedule 4, Part 2 of the Bill would require ASIO to notify the IGIS where certain SCSAs and security clearance decisions (SCD) are not furnished or made within 12 months. While SCSAs and SCDs were not part of the ASIO Act at the time the Comprehensive Review was released, given the equivalent functionality, it is appropriate to include a similar notification scheme for SCSAs and SCDs in the new Part IVA of the ASIO Act.

16. Consistent with the Government response to the Comprehensive Review, the amendments do not require ASIO to notify the *subjects* of certain delayed SAs, SCSAs and SCDs, as recommended by the Comprehensive Review. The amendments have been developed in consultation with ASIO to ensure an appropriate balance between ASIO being accountable for delays, and the interests of security. Given the proposed amendments would require ASIO to report these matters to the IGIS, the Department considers there is no clear additional benefit to be drawn from requiring ASIO to notify an individual of their right to make a written complaint to the IGIS, as originally proposed by Recommendation 199. The same effect can be achieved through administrative changes to relevant forms or guidance material.

17. The Department also notes that Schedule 1 Part 3 and Schedule 4 Part 2 include an exception to the requirement to notify the IGIS in relation to ASIO-initiated SAs, SCSAs and SCDs. This exception accounts for circumstances where ASIO may, in the course of its activities, self-initiate enquiries to determine if further action is required, on its own motion. As this would be done internally, without the subject being aware, the Department's view is the assessment would not be delayed from the perspective of the subject and it is therefore not necessary for a notification to be made. The oversight of the IGIS is not diminished, as irrespective of this exception, the IGIS may request to inspect ASIO initiated SAs, SCDs and SCSAs at any time.

Schedule 2 – Protecting identities and information

2.1. Schedule 2, Part 1 – Cover employment

18. Schedule 2, Part 1 of the Bill would implement recommendation 70 and 71 of the Comprehensive Review by protecting current and former ASD, ASIO and ASIS employees and affiliates from criminal liability when identifying a specified authority of the Commonwealth as their employer.

19. This part would amend the ASIO Act and IS Act to enable current and former ASD, ASIO and ASIS employees and affiliates to identify an authority of the Commonwealth as the person's employer or place of work, where the authority has been determined by the Director-General of Security, ASIS or ASD respectively. Persons using cover employment, or facilitating cover under these arrangements, would be protected from criminal liability if done in the proper performance of that person's powers, functions or duties, or in their professional capacity.

20. These amendments are required to formalise and update existing cover arrangements for ASD, ASIO and ASIS where it would be inappropriate for current and former ASIO employees and affiliates to identify ASD, ASIO and ASIS as their employer for security reasons. Limiting the protection from criminal liability to being available only in relation to identifying an authority of the Commonwealth as their employer, and then only in the course of the proper performance of an individual's duties or professional capacity, ensures this protection is tightly defined.

2.2. Schedule 2, Part 2 – Consolidating secrecy offences

21. Schedule 2, Part 2 of the Bill would implement recommendation 143 of the Comprehensive Review. It consolidates the secrecy offences contained in Division 1 of Part 6 of the IS Act. These amendments increase the protection of identity of staff members of agencies that are regulated by the IS Act. Additionally, these amendments would reduce the number of secrecy offences in Commonwealth laws, consistent with the Attorney-General's recently released Review of Commonwealth Secrecy Offences. By consolidating these offences, it would reduce the ability to identify the precise agency to whom the conduct giving rise to the offence relates, affording greater protection to agencies and their employees. The Department notes that it is not intended for these amendments to alter, or otherwise affect, the scope of these secrecy offences. Further, consistent with the status quo and principles of open justice, the consolidated offences do not prevent the identity of an accused or the fact that they have been charged from being made public.

2.3. Schedule 2, Part 3 – Protection from disclosure under the Archives Act 1983

22. Schedule 2, Part 3 of the Bill would implement recommendation 190 of the Comprehensive Review. The amendments would change the AAT Act and the Archives Act to ensure the identity of current and former ASIO and ASIS employees, affiliates, staff members and agents that are included in Commonwealth records and are in the 'open access period' are protected from public access and disclosure.

23. While the identities of ASIS and ASIO staff members and agents are currently able to be exempted from disclosure on security grounds, an express exemption in the Archives Act would clarify the protected status of ASIO/ASIS identities and better align with publication offences contained in the IS Act, the ASIO Act and other Commonwealth legislation.

2.4. Schedule 2, Part 4 – Protecting the identity of ASIO employees and ASIO affiliates

24. This amendment would strengthen the protection of identities of ASIO employees or ASIO affiliates, by modernising the publication offence under section 92 of the ASIO Act.

25. Section 92 currently makes it an offence for a person to publish, including through various means, any matter stating, or from which it could reasonably be inferred that a person is a current or former ASIO employee or affiliate, or is in any way connected with an ASIO employee or affiliate, without the consent of the Minister responsible for ASIO or the Director-General of Security.

26. These amendments remove references to specific publication methods to ensure the section remains appropriate into the future. In an increasingly interconnected world, publication can occur in many ways, and new publishing platforms regularly emerge. It is therefore necessary to update the offence to prohibit the publication of information identifying an ASIO employee or affiliate regardless of the publishing platform. The amendment also provides for a number of exceptions:

    a. Where the Minister responsible for ASIO or the Director General of Security has consented in writing to the information being made public.

    b. Where a former ASIO employee or affiliate has consented in writing to their identity being made public, or otherwise caused or authorised their identity to be made public by the third person. This exception would protect third parties who act in reliance on advice from former ASIO employees and affiliates, while clarifying that former officers themselves cannot rely on this exception.

27. The amendments also introduce a new disclosure offence for ASIO identities, in certain circumstances, at section 92A. This proposed offence has a high threshold to be met in order for the offence to apply; a defendant must have intended to, or knew that a disclosure would, endanger the health or safety of a person, or prejudice the effective performance of the functions or duties, or the effective exercise of the powers of ASIO. The amendment requires that a prosecution can only be instituted by, or with the consent of, the Attorney-General.

28. The Department also notes the amendments align with 9 of 12 principles for framing secrecy offences set out in the Review of Commonwealth Secrecy Offences. The amendments do not align with two of the principles and one of the principles is not applicable.

    a. The amendments do not align with Principle 6 'Secrecy Offences should clearly identify any third parties regulated by the offence and separate offences should apply to third parties' and Principle 7 'Offences capturing third parties should have a higher threshold for establishing criminal liability'. The ASIO Act offences do not treat third parties separately as ASIO staff members should not be exposed to harm by virtue of their association with ASIO, regardless of who makes the association public.

    b. Principle 12 'All Commonwealth departments and agencies should regularly review specific secrecy offences in legislation they administer as part of reviews of legislation and legislative instruments,' is not applicable.

Schedule 3 – Authorisations for intelligence activities

3.1. Schedule 3, Part 1 – Sequencing of ministerial authorisations and clarifying references to persons

29. Schedule 3, Part 1 would implement recommendation 2 of the Comprehensive Review by amending the IS Act to enable a Minister to give an authorisation to ASIS, AGO or ASD to undertake certain activities in respect of Australian persons, in circumstances where the Australian persons are, or are likely to be, involved in activities that are, or are likely to be, a threat to security or, involved with a listed terrorist organisation, and *then* obtain the agreement of the Attorney-General. The authorisation cannot take effect unless and until the agreement of the Attorney-General has been obtained.

30. This part would also amend the IS Act to clarify that a Minister may give an authorisation to ASIS, AGO or ASD to undertake such activities, in circumstances where Australian persons are involved in activities that present a significant risk to their own safety, or are themselves involved in activities relating to the contravention, or alleged contravention, of a UN sanction enforcement law.

31. The amendments provide for greater flexibility by enabling either the relevant Minister, or Attorney-General, to first authorise or agree to the activity, while still ensuring both authorisation and agreement are in place before it takes effect. The 2017 Independent Intelligence Review and the Comprehensive Review both noted the current sequencing of the IS Act ministerial authorisation regime — which specifies the Attorney-General's agreement must be obtained first — could be altered to provide for the Attorney-General's agreement to be sought either before or after without taking away from the importance of the Attorney-General's role in the authorisation process.

32. The Department notes that the amendment does not change the Attorney-General's essential role in the IS Act ministerial authorisation regime. Ministerial Authorisations in relation to persons engaging in threats to security will still require the Attorney-General's agreement before coming into force. Questions going to the appropriateness of a ministerial authorisation are matters for the minister responsible for the IS Act agency, with the Attorney-General's role being to agree to the ministerial authorisation.

3.2. Schedule 3, Part 2 – References to Attorney-General not to include junior minister

33. Schedule 3, Part 2 would implement recommendation 17 of the Comprehensive Review by amending the ASIO Act and the TIA Act to provide that the powers vested in the Attorney-General may only be exercised by the Attorney-General and not a junior minister within the portfolio. These amendments are not intended to prevent a person who is acting as the Attorney-General to exercise those powers.

34. The Department notes the issuing of an ASIO warrant by a junior minister is a fundamental departure from the principles underpinning the ministerial warrant framework. The ability for junior ministers to issue ASIO warrants effectively 'bypasses' the Attorney-General's role as First Law Officer. This would risk damaging the public confidence in the level of control over ASIO's activities and ultimately, the legitimacy of the control framework.

35. The Department notes that it is already a matter of practice that the powers vested in the Attorney-General in respect of ASIO are not exercised by junior ministers. However, given the importance of ministerial oversight of intelligence agencies, the Department's view is there is merit in explicitly according these powers to the Attorney-General alone.

36. The Department notes that removing the Director-General of Security's ability to request a junior minister to issue a warrant is not expected to result in any undue delays or difficulties for ASIO, including because there are separate provisions for the issuing of warrants in emergency circumstances.

3.3. Schedule 3, Part 3 – Applicant for special intelligence operation activity

37. Schedule 3, Part 3 would implement recommendation 68 of the Comprehensive Review by amending the ASIO Act to provide that only the Director-General of Security may apply to the Attorney-General for an authority to conduct a special intelligence operation.

38. These amendments align the persons who can apply to the Attorney-General for a special intelligence operation with those who can request special powers warrants and questioning warrants elsewhere under the ASIO Act. Given that a special intelligence operation authorisation empowers ASIO to undertake an activity, or activities, which would otherwise be unlawful, it is more appropriate for only the Director-General to be able to apply for a special intelligence operation authorisation. Conferring the power to apply for a special intelligence operation to only the Director-General also strengthens the safeguards around ASIO's use of special powers operations.

39. The Department notes that these amendments are not expected to adversely impact ASIO's operational flexibility.

Schedule 4 – Security vetting and security clearance related activities

4.1. Schedule 4, Part 1 – Security clearance suitability assessments

40. Schedule 4, Part 1 of the Bill would amend the ASIO Act to clarify the definition of terms used in that Act and enable the Director-General of Security to delegate their power or function to furnish non-prejudicial security clearance suitability assessments (SCSA) to an ASIO employee or affiliate irrespective of what position within ASIO the person holds.

41. These amendments will ensure the effective operation of ASIO's security vetting and security clearance related functions, while ensuring delegations remain commensurate with their impact on a clearance subject. As non-prejudicial SCSAs do not have an adverse impact on clearance subjects, non-prejudicial SCSAs being delegable to any appropriate officer, as opposed to the existing EL1 or higher delegation for prejudicial SCSAs, is appropriate.

42. The Department does not believe that the amendment risks reducing the strength of the oversight framework for ASIO's SCSAs. The exercise of the power or function to furnish prejudicial SCSAs remains with an EL1 or higher officer, noting such an outcome may have an adverse impact on the subject. Where SCSAs are prejudicial, subjects' eligibility for certain roles can be curtailed, or their ability to continue to hold their existing role could be jeopardised, and retaining a higher delegation is appropriate. With limited exception, such assessments are reviewable in the AAT.

    a. The Department notes ASIO can be expected to continue to maintain appropriate internal management, oversight and scrutiny of its SCSA processes, including in relation to non-prejudicial decisions. Employees and affiliates who may exercise the power or function, regardless of substantive position, can be expected to have suitable training and experience to make non-prejudicial decisions, proportionate and appropriate to the significance of the decision being made.