Australian Government
Australian Security Intelligence Organisation

ASIO submission to the Parliamentary Joint Committee on Intelligence and Security

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

February 2024

75
1949–2024

ASIO

Remembering the past, securing the future

Vladimir Petrov defecting at Sydney Airport, 3 April 1954.

Introduction

1. The Australian Security Intelligence Organisation (ASIO) welcomes the opportunity to make this submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) for its Review of the National Security Legislation Amendment (Comprehensive Review and Other Measures No. 3) Bill 2023 (the Bill). The Bill includes amendments to implement a number of recommendations of the Comprehensive Review of the Legal Framework of the National Intelligence Community (the Comprehensive Review) and a small number of additional amendments, which include measures to strengthen protections of the identities of ASIO employees and affiliates.

2. This submission addresses the following measures that relate to ASIO:
    - Identity protections for ASIO employees and affiliates through cover employment, protection from disclosure under the Archives Act and strengthening identity disclosure offences in the ASIO Act (Schedule 2 Parts 1,3 and 4); and
    - Security Assessments, security vetting and security clearance related decisions (Schedules 1 and 4).

Identity protections (Schedule 2 Parts 1, 3 and 4)

3. The publication or disclosure of the identity of a current or former ASIO employee or ASIO affiliate has the potential to cause grave harm to security. Release of the identity of ASIO employees or ASIO affiliates would substantially increase the risk they will be targeted by hostile third parties to undermine Australia's security and put the lives of ASIO employees and affiliates, as well as their families, at risk.

4. We need to make sure we protect our staff, and their ability to protect our sensitive capabilities and operations. As the Director-General of Security stated in his 2023 Annual Threat Assessment:

    "We must protect our people: our staff are undeclared for their safety. Spies want to target them and extremists want to kill them. The machete hanging on the wall of one of our buildings is an ugly reminder of this reality—an extremist plotted to use it on one of our officers."

5. Disclosure of the identity of ASIO employees or ASIO affiliates can also degrade the effective performance of ASIO's functions, duties or powers, and adversely affect the careers of those employees or affiliates. ASIO, therefore, strongly supports the measures in the Bill that ensure protections for the identity of ASIO employees and affiliates remain robust in the face of the changing security environment.

Strengthening identity disclosure offences in the ASIO Act

6. Section 92 of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) makes it an offence to publish or otherwise make public the identity of current or former ASIO employees and affiliates. That offence was implemented in response to a campaign of harassment against ASIO staff following the Murphy raids on ASIO offices in 1973.

7. Following the Murphy raids in 1973, a Victorian activist began 'nuisance operations' against ASIO and its staff, which included television and radio appearances calling for the abolition of ASIO. Throughout 1973-1976, multiple ASIO officers were subjected to harassment by activists. The activities against ASIO staff included being photographed, being followed, being subjected to harassing telephone calls, being identified as ASIO officers in publications, being confronted at their

homes, having their home and car door locks tampered with, and intimidating hoax calls being made (including bomb threats). This campaign also had an adverse effect on their families.

8. Disclosure of the identity of an ASIO employee or affiliate could hamper their ability to carry out their covert duties; this could damage ASIO's ability to perform its functions. In addition, ASIO employees and affiliates continue to face great personal risk, including risk to life, if their identities are made public, published or inappropriately disclosed.

9. The section 92 offence references methods of publication that have failed to keep pace with the introduction of modern forms of publication and communication. The amendments in the Bill would ensure the publication offence remains current by removing references to specific publication methods, so that the offence will apply regardless of the means by which the information is made public.

10. The Bill would also introduce a new offence that prohibits the disclosure of the identity of an ASIO employee or ASIO affiliate where the person intended or knew that the disclosure would endanger the health or safety of a person, or where they intend to prejudice the effective performance of ASIO's functions. This offence brings protections for the identity of ASIO employees and affiliates into closer alignment with other intelligence staff under section 41 of the *Intelligence Services Act 2001.*

Cover employment

11. To protect the identities of our staff, ASIO employees and affiliates need to use cover arrangements to avoid disclosing their connection with ASIO in some circumstances. The proposed amendment formalises and updates existing cover arrangements. It will enable ASIO employees and affiliates to identify another Commonwealth authority as their employer or place of work where it would be inappropriate, for security reasons, to identify ASIO as their employer or place of work.

Relevant findings of the Comprehensive Review

12. The Comprehensive Review recommended that:

    - Recommendation 71: The Australian Security Intelligence Organisation Act should be amended to provide that the Director-General of Security can authorise the use of a Commonwealth department or agency as the cover employer for ASIO employees and affiliates.

Protection from disclosure under the Archives Act

13. Disclosure of the identity of an ASIO employee and affiliate, or an ASIS staff member, has the potential to cause grave harm to security and put the individual and those connected to them at risk even decades after a relevant record was created.

14. While the identities of ASIO and ASIS staff are exempt from being disclosed when records are released under the *Archives Act 1983* (Archives Act) where it would be prejudicial to security, ASIO would welcome the proposed express exemption to put beyond doubt the parliament's intention that ASIO and ASIS identities not be disclosed through release of records under the Archives Act.

Relevant findings of the Comprehensive Review

15. The Comprehensive Review recommended that:

    - Recommendation 190: The identities of ASIO and ASIS staff members and agents should be protected from disclosure under the Archives Act.

Security assessments (Schedules 1 and 4)

Prescribed Administrative Action

16. ASIO welcomes amendments to Part IV of the ASIO Act that refine the framework for security assessments by clarifying the definition of 'prescribed administrative action' (PAA). By specifying which administrative decisions are considered to be prescribed administrative action, ASIO would have certainty about when security advice is required to be given in the form of a security assessment. ASIO is not currently aware of any actions that would be added to the definition of PAA through regulations.

17. The Bill would extend the definition of PAA to explicitly include the exercise of powers or functions in relation to parole, security guard licenses and firearms licences. The amendments would ensure an individual affected by a decision about their parole, or their suitability to hold firearms or security guard licences, is entitled to the notice and review rights under Part IV of the ASIO Act. The amendments also provide for circumstances in which ASIO may communicate information not amounting to a security assessment relating to these decisions.

18. The Bill would also clarify that a decision under the *Foreign Acquisitions and Takeovers Act 1975* does not constitute PAA, which has the effect of exempting ASIO assessments provided for the purpose of informing such decisions from the operation of Part IV of the ASIO Act

Relevant findings of the Comprehensive Review

19. The Comprehensive Review recommended that:

- Recommendation 193: The definition of 'prescribed administration action' in the Australian Security Intelligence Organisation Act should be amended to include the exercise of powers or functions in relation to parole, security guard licences and firearms licences.
- Recommendation 194: A regulation making power should be inserted into the definition of 'prescribed administration action' in the Australian Security Intelligence Organisation Act.
    i. 194.a The regulation making power should allow regulations to add an action to the definition of 'prescribed administrative action' where that action has potential to affect an individual's liberty or livelihood. Matters relating to security would be a key consideration in taking that action.
    ii. 194.b Regulations made under the regulation making power should be reviewed by the PJCIS before the end of the applicable disallowance period in each Chamber prior to coming into effect.
- Recommendation 197: ASIO security assessments prepared for the purpose of informing the Foreign Investment Review Board should be exempted from the operation of Part IV of the Australian Security Intelligence Organisation Act.

Preliminary communication to Commonwealth agencies, states and territories or authorities of a state or territory

20. ASIO supports the amendments enabling the Organisation to communicate information to a state or territory (State), or an authority of a State (including through a Commonwealth agency), for the purpose of enabling that State or authority to take certain PAA of a temporary nature as a matter of urgency, pending the furnishing of a security assessment.

21. This replicates the current arrangement for Commonwealth agencies and removes a barrier to the State or authority of a State from taking temporary, urgent action where the requirements of security make it necessary.

Relevant findings of the Comprehensive Review

22. The Comprehensive Review recommended that:

    - Recommendation 198: The Australian Security Intelligence Organisation Act should be amended to allow ASIO to make a preliminary communication directly to a state or territory agency where the requirements of security make it necessary, as a matter of urgency, to take action of a temporary nature pending the furnishing of a security assessment.

Inspector-General of Intelligence and Security notification of delayed assessments and decisions

23. The Bill amends the ASIO Act to require the Director-General of Security to notify the Inspector-General of Intelligence and Security (IGIS) of certain security assessments, security clearance decisions and security clearance suitability assessments that are not furnished within 12 months after ASIO starts to prepare the assessment or decision, in accordance with a written protocol.

24. The proposed amendments proactively extend the notification requirements recommended by the Comprehensive Review to include security clearance decisions and security clearance suitability assessments recently introduced by the *Australian Security Intelligence Organisation Amendment Act 2023*.

25. The protocol would specify the period in which notification of a delayed assessment or decision must be made, and the information to be included in the notification. These matters will necessarily engage questions of ASIO's internal processes and procedures, which are classified. It is therefore necessary they be included in the protocol and not made public or set out in legislation.

26. The protocol would provide mechanisms to ensure that the IGIS is notified of any delayed assessments or decisions, but would not compel ASIO to re-prioritise, or rectify any aspect of, those cases which are delayed.

27. ASIO already maintains internal processes for prioritising and managing cases where a security assessment, security clearance decisions or a security clearance suitability assessment is required. ASIO's processes and management of these cases are already subject to oversight by the IGIS.

28. ASIO welcomes robust oversight provided by the IGIS, which supports ASIO's commitment to legality and propriety. Noting the IGIS currently has oversight of ASIO's work on security assessments, this measure would serve to prompt proactive reporting by the Organisation.

Relevant findings of the Comprehensive Review

29. The Comprehensive Review recommended that:

    - Recommendation 199: The Australian Security Intelligence Organisation Act should be amended to require ASIO to notify the IGIS in every instance where it has taken more than 12 months to finalise a security assessment, and subject to the requirements of security, notify the individual in writing of their ability to make a written complaint under the Inspector-General of Intelligence and Security Act. If the requirements of security do not permit notification of the individual, IGIS must be notified of this fact.

Supporting quicker processing of non-prejudicial security clearance suitability assessments

30. The Bill amends the ASIO Act to support quicker processing of non-prejudicial security clearance suitability assessments by enabling the Director-General of Security to delegate their power or function to furnish such assessments to an ASIO employee or ASIO affiliate, irrespective of what position within ASIO the person holds.

31. ASIO supports these amendments, which are essential to ensure the effective operation of ASIO's security vetting and security clearance related functions, taking into account the anticipated high volume of security clearance suitability assessments, while ensuring delegations remain commensurate with their impact on a clearance subject.

32. Employees and affiliates exercising the delegated function or power, 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.

33. The existing requirement for appropriate executive level approval of prejudicial security clearance suitability assessments would be unchanged.