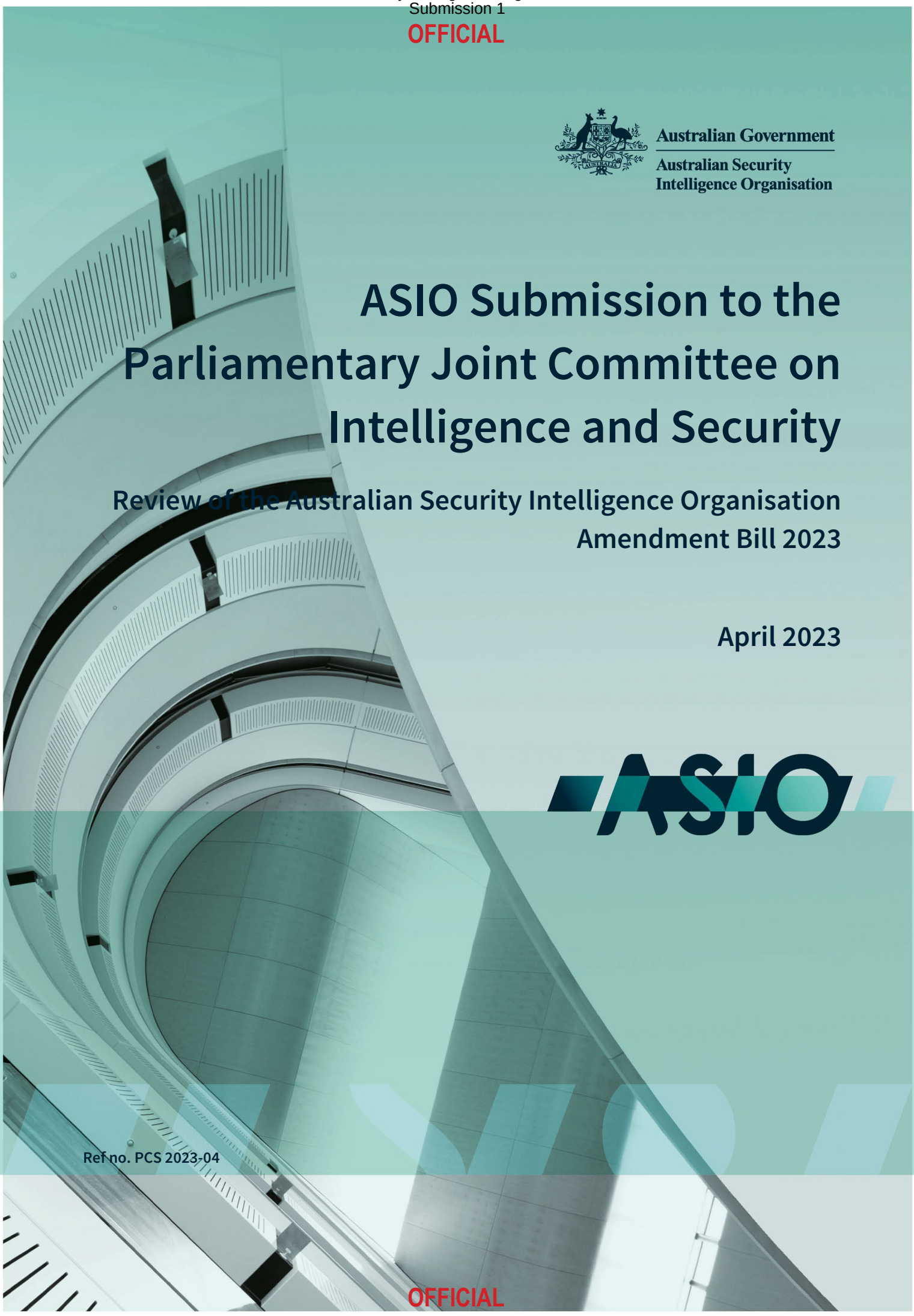
Australian Government
Australian Security Intelligence Organisation

ASIO Submission to the Parliamentary Joint Committee on Intelligence and Security

Review of the Australian Security Intelligence Organisation Amendment Bill 2023

April 2023



Ref no. PCS 2023-04

Part 1 – Introduction

Overview

1. The Australian Security Intelligence Organisation (**ASIO**) welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Intelligence and Security's review of the Australian Security Intelligence Organisation Amendment Bill 2023 (the **Bill**).
2. The reforms in the Bill are designed to enable Australia to respond to a security environment that is complex, challenging and changing. It is critically important the Australian Government's most privileged information, capabilities and secrets are protected. It is equally vital the Australian Government's most highly cleared workforce is responsive and mobile enough to be directed to where the Government needs it most.
3. In this context, the Bill contains a suite of amendments to:
   - uplift and harden Australia's highest level of security clearance in response to the unprecedented threat from espionage and foreign interference; and
   - improve interoperability and burden sharing as the Australian Government delivers critical national security capabilities.
4. The proposed amendments would enable ASIO to be centrally responsible for the issue and maintenance (ensuring the ongoing suitability of a person to hold a security clearance) of a new security clearance—the TOP SECRET-Privileged Access (**TS-PA**) security clearance—which over time will replace the existing Positive Vetting (**PV**) security clearance. TS-PA security clearances are governed by a new, classified TS-PA Standard, which establishes stronger minimum mandatory security clearance requirements reflecting contemporary psychological and insider threat research.
5. The PV operations of those agencies authorised to issue and maintain PV security clearances for their own personnel or others—ONI, the Australian Secret Intelligence Service (**ASIS**), the Australian Federal Police (**AFP**), and the Australian Government Security Vetting Agency (**AGSVA**)—will be transitioned to ASIO in phases. AGSVA will remain responsible for most lower-level security clearances, from Baseline to Negative Vetting Level 2.
6. Centralising Australia's highest-level security clearance vetting in ASIO leverages ASIO's security intelligence functions, holdings and capabilities to allow a holistic assessment of a person's suitability to hold such a clearance, having regard to the most current and accurate information about the security threats confronting Australia.
7. The Bill would also enable the ongoing operation of a Quality Assurance Office (**QAO**) in the Office of National Intelligence (**ONI**). The QAO will independently assure the quality, consistency and transferability of TS-PA security clearances, and drive the uplift of an insider threat capability across those Commonwealth entities sponsoring TS-PA security clearances.
8. The reforms in the Bill reflect that security clearance processes are subject to the voluntary participation by clearance applicants. ASIO would only exercise its new security vetting function in respect of individuals who have applied for, or who hold, a security clearance. Applicants will be required to give clear and informed consent to the collection, use and disclosure of their personal information and are provided with a clear understanding of how that information will be used.

Background to the reforms

9. On 1 July 2020 a multi-agency Future Positive Vetting Capability Taskforce was established to modernise whole-of-government vetting standards to enable increased consistency, heightened assurance and transferability of Australia's highest-cleared workforce.
10. The Taskforce developed a suite of reforms to incrementally replace the current PV clearance. This included the development of the new classified TS-PA Standard, and through it, the TS-PA security clearance, which was

subsequently established under the Protective Security Policy Framework (PSPF). The National TS-PA Capability was established on 1 December 2021.

11. The threat of espionage and foreign interference, and the opportunity costs to the Australian Government of not having a transferable highest-cleared workforce, are the genesis to the reforms outlined. The threats we face and the individual nature of security clearance decisions requires time to make the right call. The reforms are being undertaken to strengthen assurance and consistency, and therefore improve the movement of already cleared staff across government.

Part 2 – Threat, consistency and transferability

Threat environment

12. Australia's security environment is complex, challenging and changing. Espionage and foreign interference are Australia's principal security concern. More Australians are being targeted by hostile foreign powers and their proxies (FPP) than at any time in Australia's history.

13. Hostile FPPs are aggressively seeking secrets across all parts of Australian society. They are targeting our security-clearance holders, those with access to Australia's most privileged information, capabilities and secrets. Since the announcement of AUKUS, there has been a distinct uptick in the online targeting of people working in Australia's defence industry. Regardless of who is being targeted, and regardless of how—whether online or in person—the intent is the same. Hostile FPPs are trying to develop relationships they can exploit.

14. The legitimate access which trusted insiders have provides opportunities for the unauthorised removal of information, the facilitation of technical operations, and the influence to obtain favourable outcomes. We must therefore ensure that our trusted insiders can be and remain trusted—ASIO is uniquely placed to do that.

15. The threat of hostile FPPs to Australian Government personnel across Parliament, Commonwealth employees and the APS, Defence and separately the judiciary—is genuine and where realised can cause grave harm to Australia's nation interests. Hostile FPPs will continually seek to test the clearance system, seeking to put in place disloyal persons with access to classified and privileged information. As such, the personnel and systems will themselves continue to be a focus of hostile FPP activity.

16. Whether it is information from Australia's intelligence community or our Five-Eyes partners, about Australia's ground-breaking nuclear-powered submarines program with US and UK partners, or other advanced defence and intelligence capabilities, Australia's sovereignty demands that Australia's most sensitive information, capabilities and secrets be protected. The reforms in the Bill would help harden and uplift Australia's security clearance process to address these threats.

Need for consistency and transferability

17. There are presently five separate vetting agencies authorised to grant PV security clearances. This model has resulted in different applications of policy and standards aligned to individual missions and requirements rather than a consistent and coordinated approach to PV security vetting. This is because agencies:

- operate across multiple Commonwealth portfolios
- work to different missions and priorities, and
- operate under different workforce considerations and risk profiles.

18. As a result of these differing processes, there have been barriers for agencies seeking to recognise a PV clearance granted by another authorised vetting agency. This has resulted in delays in transferring clearances between agencies, impeding the mobility of highest-cleared personnel across government. In implementing a single TS-PA Standard, and a clearance issued and maintained in a uniform manner by a centralised authority, ASIO is creating a consistent and quality assured security clearance, the sponsorship of which can be readily transferred across government to respond to changing priorities.

Part 3 – Operational imperatives

19. The Bill would provide ASIO with a new security vetting and clearance related function; enable the freer exchange of information between ASIO and sponsors to manage and mitigate security risks; and introduce a new review framework to ensure accountability of ASIO decisions and assessments.

20. Without these reforms, ASIO would not be able to make security clearance decisions for clearances sponsored by other agencies. The continued application of Part IV of the ASIO Act to security vetting and clearance related communications would limit the ability of ASIO and sponsors to identify, manage and mitigate security threats. Further, review rights for ASIO security clearance decisions and assessments would remain fragmented and inconsistent across those affected by them.

The need for a new function for ASIO

21. The Bill would amend the ASIO Act to introduce a new function (proposed paragraph 17(1)(cb)) and a new Part IVA into the ASIO Act which provides that ASIO may:

    - make security clearance decisions and to undertake security vetting, including on an ongoing basis, for ASIO and non-ASIO personnel alike;
    - communicate with a sponsoring agency for a security clearance in relation to the ongoing suitability of a person to hold the security clearance to facilitate a stronger and more effective partnership and shared responsibility between ASIO and the insider threat capabilities of sponsoring agencies; and
    - provide security clearance suitability assessments to other vetting agencies to inform security clearance decisions made by those agencies—this replaces, but is consistent with, the security assessment framework in Part IV of the ASIO Act to the extent it covers security vetting and clearance related communications.

22. ASIO's current function in subsection 17(1)(c) of the ASIO Act is limited to providing *advice*, and does not extend to making security clearance *decisions* in relation to security clearances sponsored by other agencies. Enshrining in legislation ASIO's ability to perform security vetting on an ongoing basis, and to communicate with sponsors about security clearance suitability more freely than is presently the case, will ensure proper legal authority subjected to Parliamentary oversight.

23. The Bill would enable the Director-General of Security to delegate these new functions to ASIO employees and affiliates. This ensures government agency secondees to ASIO, and contractors engaged by ASIO for security vetting purposes—and who are subject to the same standards, policies and procedures as ASIO employees—are able to undertake security vetting and security clearance related activities on ASIO's behalf. This will maximise ASIO's ability to exercise its new security vetting and clearance functions to meet forecast demand by drawing on experienced and skilled practitioners from within and outside of ASIO in specific and controlled circumstances. Contractors or human sources acting as ASIO affiliates will not be permitted to make security clearance decisions and provide security clearance suitability assessments to other authorised vetting agencies on ASIO's behalf.

24. ASIO activities are further bound by the Minister's Guidelines, which are applicable to both ASIO employees and affiliates. The Guidelines include a number of requirements relating to ASIO's treatment of personal information, including that ASIO's collection, retention, use, handling and disclosure of personal information is limited to what is reasonably necessary to perform its function.

25. Delegations to make security clearance decisions and to provide security clearance suitability assessments may only be to at least EL1 equivalent (proposed subsection 16(1C)). A higher delegation floor would impede ASIO's ability to make decisions or provide assessments in a timely manner. However, more complex cases, or cases that involve prejudicial decisions or assessments, would generally be escalated to more senior delegates, with the seniority of the escalation depending on the complexity and sensitivity involved.

The need for a freer flow of information

26. Proposed section 36A of the Bill would disapply the operation of Part IV of the ASIO Act (except for section 81), to the extent it relates to the exercise or performance of a power or function under Part IVA. This would enable ASIO and security clearance sponsors to share information more freely about a person's suitability to hold a security clearance. This facilitates a stronger and more effective partnership between ASIO and the insider threat capabilities of the agencies which sponsor security clearance holders, recognising security is a shared responsibility. The freer flow of information would also enable an integrated, single repository of information about security clearance holders. This is critical to enabling the ongoing, rather than point-in-time, validation of an individual's suitability for a security clearance.

27. Part IV of the ASIO Act currently prohibits Commonwealth agencies from taking permanent prescribed administrative action on the basis of ASIO advice, unless that advice is a security assessment (section 39 of the ASIO Act). Relevantly, prescribed administrative action includes (in broad terms) action that *relates to or affects* access to places or information controlled or limited on security grounds – this includes actions affecting security clearance holders and applicants. Subject to limited exceptions, prejudicial security assessments are reviewable in the Administrative Appeals Tribunal (AAT).

28. The current Part IV requires that information to be shared with clearance sponsors be done so through a security assessment—that is, in practice, a formal, exhaustive examination set out in a prescribed format and which is approved by the Director-General of Security in each instance. In doing so, Part IV impedes ASIO's ability to share clearance suitability information with sponsors early, and often, to proactively manage insider threats and other risks. As changes in an individual's suitability go unreported—and without the ability to communicate more freely with clearance sponsors—risks accumulate. Periodic revalidation not supported by a continuous exchange of clearance suitability information makes the aggregate of individual unreported changes more difficult to manage, and may in extreme cases result in a clearance subject being found no longer suitable only after a significant risk has materialised.

Part 4 – Accountability and new rights of review

29. ASIO's security vetting will be both rigorous and reasonable. The Bill recognises the impact a prejudicial security clearance decision can have on an individual, and so seeks to balance that with the likelihood hostile FPPs will use any review rights for the purpose of intelligence collection to understand the:

- extent and content of ASIO intelligence holdings, which may allow a foreign adversary to at least partially reverse engineer the nature and extent of the TS-PA security clearance process;
- methodology concerning security clearance suitability assessments: revealing how information gained through the vetting process was translated into an assessment of threat; and
- information that reveals ongoing intelligence coverage of associates of the applicant, disclosure of which could prejudice security.

30. Hostile FPPs would be able to use this understanding to 'game the system'—that is, to send applicants to apply for, and gain, TS-PA security clearances to then infiltrate Australian Government agencies providing access to the highest levels of Australian, and allied, information, capabilities and secrets.

31. The approach proposed, therefore, distinguishes between existing clearance holders and new clearance applicants; providing tailored avenues of review for each. This recognises that the threat of espionage and foreign interference is higher for new applicants who have not yet participated in security awareness training and who have only a rudimentary understanding of security obligations, and who are therefore less able to manage the threats posed by hostile FPPs or who are more susceptible to being duped or exploited by an FPP. New applicants also bring a lower level of assurance as they do not have existing track records as Commonwealth employees.

Inspector-General of Intelligence and Security

32. The Bill would maintain the IGIS's existing oversight role of ASIO and ONI. The IGIS remains responsible for investigating complaints and reviewing the activities of both agencies, ensuring they act legally and with propriety, comply with Ministerial guidelines and directives, and respect human rights. The IGIS reports annually to Parliament on their oversight of ASIO and other agencies. The IGIS will continue to be able to undertake inquiries at their own volition, or in response to complaints or at the request of the Attorney-General or responsible Minister.

33. The IGIS's remit would not extend to review of those ASIO security clearance decisions and security clearance suitability assessments that under the Bill would be eligible for review in the AAT (or in due course its successor body), as the AAT provides an independent and impartial review pathway for such decisions and assessments. This reflects an existing exception in section 9AA(c) of the *Inspector-General of Intelligence and Security Act 1986*, which precludes the IGIS from reviewing matters reviewable in the Security Division of the AAT.

Quality Assurance Office in the Office of National Intelligence

34. The Bill would provide ONI with a new function to provide quality assurance, reporting and advice in relation to TS-PA security clearances issued by ASIO, and to assist Commonwealth authorities that sponsor those clearances to establish and maintain those authorities' capability to prevent and detect insider threats (proposed paragraph 7(1)(ba) to the *Office of National Intelligence Act 2018* (**ONI Act**)). The Bill would ensure existing limitations in the ONI Act do not preclude the QAO from undertaking its functions (proposed subsection 10(2A) to the ONI Act).

New rights of review

35. Under Australia's current Commonwealth security clearance framework, there are no statutory rights to seek internal or external merits review of security clearance decisions made by authorised vetting agencies. There are limited rights in Part IV of the ASIO Act for certain persons to seek review of adverse or qualified security assessments that may be used by vetting agencies to inform their security clearance decisions, but these do not apply to staff members of ASIO, ASIS, ONI, the Australian Signals Directorate (**ASD**), the Australian Geospatial-Intelligence Organisation (**AGO**) or the Defence Intelligence Organisation (**DIO**).

36. The Bill seeks to address this inconsistency by ensuring that ASIO's involvement in security clearance processes is accountable by providing new rights of review. These are subject to limited exceptions that balance prejudicial impacts on individuals with the need to protect the security clearance process from FPP exploitation, insider threats and other threats to their security.

Review rights of ASIO security clearance decisions

37. The Bill would establish the following merits review framework for ASIO's security clearance decisions:

- A new internal merits review framework that would enable review of prejudicial ASIO security clearance decisions (decisions to deny, revoke, or impose or vary certain conditions upon, a security clearance) by an alternate delegate within ASIO. This framework does not apply to a decision about a non-citizen or a person not normally resident in Australia who is seeking the clearance for work offshore.
- A new external merits review framework that would apply in respect of decisions that continue to be prejudicial after internal merits review, with review pathways specific to their circumstances and impact:
  - for existing security clearance holders and Commonwealth employees, the Bill would provide a right to seek review in the AAT of ASIO decisions to deny, revoke, or impose or vary certain conditions upon, a security clearance. The AAT may affirm a decision, or remit the decision back to ASIO for reconsideration and may make findings that are binding upon ASIO, and
  - for everyone else, the right to seek review by an independent reviewer appointed by the Attorney-General. The Independent Reviewer must consider whether the relevant decision was reasonably open to have been made, and provide a report to the Director-General of Security who must then decide what action to take, including whether to issue a new security clearance decision.

Review rights of ASIO security clearance suitability assessments

38. The Bill would also establish a right for certain affected persons to seek external merits review in the AAT (or in due course its successor entity) of ASIO's prejudicial security clearance suitability assessments, which are used by other security vetting agencies to inform their security clearance decisions. Such assessments are prejudicial if they contain information that would or could be prejudicial to a security clearance decision in respect of the person.

39. This review right is backed by provisions in the Bill that would have the effect of preventing other security vetting agencies from making security clearance decisions on the basis of ASIO advice, unless that advice is in the form of a security clearance suitability assessment (proposed sections 82E and 82F). Exceptions apply enabling vetting agencies to make temporary decisions to suspend, or impose or vary conditions on, security clearances in urgent circumstances.

Applicants must be provided with information

40. The Bill would mandate that persons are given reasons for a prejudicial security clearance decision or prejudicial security clearance suitability assessment made in respect of them. For security clearance decisions this is contained in proposed subsections 82J(1) and 82L(5), and for security clearance suitability assessments this is proposed section 82G. These reasons must also contain information on the review rights available to them (proposed subsections 82J(2), 82L(6), 82L(6A) and 83A(2)).

Review exceptions and information protection provisions

41. The Bill includes exceptions to review rights and information protection provisions to balance safeguards for individuals with security considerations. It does this in two ways:

- First, by limiting access to external merits review through the AAT for the following cohorts:
  - non-Australians and non-residents engaged (or proposed to be engaged) for duties outside Australia (proposed subsections 82H(3), 83(3) and 83EA(2)). This reflects the existing exception to review rights for security assessments in paragraph 36(1)(a) of the ASIO Act;
  - individuals who are neither existing clearance holders nor Commonwealth employees, who are instead provided with an avenue to independent review (proposed section 83EA); and
  - individuals whose access to external review, in exceptional circumstances, the Minister for Home Affairs determines would be prejudicial to security (proposed section 83E).
- Second, by providing mechanisms that would enable better protection of sensitive information, including:
  - the Director-General of Security and the Minister for Home Affairs being able to withhold information from the applicant, including where it would be prejudicial to security or would disclose the standard relating to Australia's highest level of security clearance (proposed ASIO Act subsections 82J(4), 82L(8), 83A(4) and 83C(5) and (6), and *Administrative Appeals Tribunal Act 1975* (AAT Act) section 38BA); (O) and
  - obligations on the AAT to withhold the standard relating to Australia's highest level of security clearance, certain information on public interest grounds (proposed AAT Act subsections 39C(3) and (4)).

Part 5 – Conclusions

42. The Bill uplifts and hardens Australia's highest-level security clearance framework in recognition that the threat of espionage and foreign interference is the highest in Australia's history. Further, by strengthening consistency and assurance, it enables transferability of already cleared staff (at the highest-level) across Government.

43. As threats to Australia evolve, so must Australia's response. We must out-think and out-manoeuvre those who seek to harm national interest; we must expand our capabilities and we must sharpen our responses.

44. At the request of the Committee, ASIO would be pleased to provide a briefing on any of the issues addressed in this submission.