HOME AFFAIRS PORTFOLIO
DEPARTMENT OF HOME AFFAIRS

PARLIAMENTARY INQUIRY SUPPLEMENTARY SUBMISSION

Parliamentary Joint Committee on Intelligence and Security

Public Hearing - 10 May 2023

Subject: Definition of Trusted Insiders

Asked by: Mrs Karen Andrews

Question: Whether a definition of a trusted insider could be provided?

Answer:

The ASIO ***Countering the insider threat*** (Attachment A), states that insiders are current or former employee or contractor who has legitimate or indirect access to a workplace's people, information, techniques, activities, technology, assets or facilities. Insiders may conduct activities that could harm a workplace, be detrimental to Australia's national security, undermine Australia's sovereignty and prosperity, or even pose a threat to life.

This is consistent with guidance on insiders provided in Policy 13 of the Commonwealth's Protective Security Policy Framework, which describes them as employees, contractors and others with access to Australian Government resources who may betray the trust placed in them by unwittingly or maliciously compromising security.

Subject: Statutory thresholds in the Bill

Asked by: Mr Andrew Wallace

Question: There are different thresholds used across the Bill, for example, the threshold for section 83A(4a) is "essential to the security of the nation" and the threshold in section 83A(4b) is "prejudicial to the interest of security". In section 83C (5)(b), the threshold is "contrary to the public interest". Why are they different statutory tests for different provisions?

Answer:

The Australian Security Intelligence Organisation Amendment Bill 2023 (the Bill) by design contains different statutory thresholds. These thresholds were developed in consultation with relevant stakeholders. The Bill recognises the impact a prejudicial security clearance outcome can have on an individual and their need to access information to understand that outcome. The Bill seeks to balance these matters with the requirements of security, including the possibility that hostile foreign powers and their proxies will exploit any review rights. Accordingly, the specifics of the statutory

threshold applied in each circumstance reflects a necessary and proportionate approach, having regard to both the requirements of security, and the impact on the applicant.

For example, in relation to security clearance suitability assessments:

- Consistent with the equivalent provision in section 38 of the ***Australian Security Intelligence Organisation Act 1979*** (ASIO Act), section 83A(4)(a) sets out that it must be '**essential to the security of the nation**' for the Minister to issue a certificate to withhold notice of a prejudicial security clearance suitability assessment from an applicant—this has the effect of preventing a person from seeking merits review. The threshold is high in recognition of the potentially adverse impact this may have. While the certificate may be subsequently revoked (s 83A(6)), in the interim the assessment may have had a significant and prejudicial impact on the affected person's livelihood and reputation.
- By contrast, section 83A(4)(b) sets out that it must be '**prejudicial to the interests of security**' for the Minister for Home Affairs to withhold from an affected person all, or part, of the statement of grounds for a prejudicial security clearance suitability assessment The ability of the Minister to withhold information that would be prejudicial to security allows the protection of the classified information included in such assessments, where security concerns would arise should the information be disclosed to the affected person.
- A different '**contrary to the public interest'** threshold applies to the ability to withhold information from a statement of grounds relating to a security clearance decision for which ASIO is responsible (paragraph 83C(5)(b)). These public interest grounds include that disclosure of the information would prejudice security, the defence of the Commonwealth or the conduct of the Commonwealth's international affairs; it would reveal information disclosed to ASIO in confidence; or it would form the basis of a claim not to disclose the information in judicial proceedings. This broader threshold applies because in those circumstances, a statement of grounds in relation to a security vetting process may contain a broader range of information that needs to be protected—not just information the disclosure of which would be prejudicial to security. For example, a statement of grounds for a security clearance decision may contain information the disclosure of which could prejudice an ongoing law enforcement investigation For the same reason, section 83C includes provisions requiring the protection of a standard relating to the Commonwealth's highest level of security clearance (paragraph 83C(5)(a)), and information that could reveal the methodology underlying a psychological assessment (paragraph 83C(5)(c)). Notably, while such information would not be given to the affected person, all information must still be given to the Administrative Appeals Tribunal (AAT) ensuring the AAT has access to all information in its review, regardless of whether it was given to the affected person.

Subject: Section 83F and Security Division of the Administrative Appeals Tribunal (AAT)

Asked by: Mr Andrew Wallace

Question: Why section 83F does not expressly state that any matters raised must be dealt with in the Security Division of the AAT?

Answer:

Referrals under s 83F are expected to be relatively uncommon and will only apply in case of special circumstance and where the affected individual cannot apply for AAT review themselves. In these circumstances, the procedures for review in the Security Division that must apply under s39A will not always be appropriate in a review referred by the Attorney-General (e.g., it may not be appropriate for the individual affected to be a party to the review).

Subsection 83F(6) provides the constitution and procedure of the AAT for proceedings under section 83F must be as determined by the President. This is consistent with section 65(2) of Part IV of the ASIO Act, which provides an equivalent power for the Attorney-General to section 83F in the context of security assessments. No provisions of the ASIO Act refer to the Security Division of the AAT.

Whether a proceeding is heard in the Security Division of the AAT is generally governed by the ***Administrative Appeals Tribunal Act 1975*** (AAT Act). However, as with section 65(2), section 83F(6) operates as a specific exception to the standard Security Division provisions in the AAT Act. This is clarified in Item 16 of the Bill, which amends section 19E(1) of the AAT Act to ensure the AAT Act exception that applies to section 65(2) also applies to proposed new section 83F.

Given that section 83F is a final safeguard allowing direct referrals by the Attorney-General, it is appropriate that the President of the AAT has the discretion to establish the constitution and procedures of the AAT to account for the specific circumstances of such hearings. However, ASIO would expect this would still involve strict protections governing the use and disclosure of security classified or other sensitive information.

Subject: Independent Reviewer

Asked by: Mr Andrew Wallace and Mr Peter Khalil

Questions: Mr Khalil and Mr Wallace asked a number of questions in relation to the independent review pathway, including ***whether existing clearance holders or Commonwealth employees should also have access to independent review and whether the proposed statutory independent review framework could cause there to be a conflict of interest in determining whether to review a case; and why the bill is silent in respect to the independent reviewer not providing information to any other unauthorised person?*** The information provided below provides the Committee with additional clarity on the independent review pathway.

The Bill currently allows, subject to limited exceptions, all affected persons to seek internal review of ASIO decisions to deny, revoke, or impose or vary conditions upon, security clearances. If the decision following internal review remains adverse, then, subject to limited exceptions:

- Affected persons who are not existing security clearance holders or Commonwealth employees (as defined in the Bill) may seek independent review of the decision by an individual appointed by the Attorney-General. The independent reviewer's opinion is then provided to ASIO, which may, but is not obliged to, make a new security clearance decision; and
- Affected persons who are existing security clearance holders or Commonwealth employees (as defined in the Bill) may seek external merits review in the AAT (and in due course, its successor body). AAT findings are binding on ASIO.

The two-stage combination of internal merits review and either independent review or external merits review in the AAT ensures that affected persons have the benefit of a multilayered and comprehensive yet efficient and effective review process that protects individual rights by ensuring access to justice, while ensuring that risks to security can be appropriately mitigated. Providing all applicants with access to an independent reviewer pathway may impact on the timeliness of the review process, including the time required for existing security clearance holders and existing Commonwealth employees/clearance holders to receive a binding review decision.

The independent reviewer pathway was developed in response to the complex, challenging and changing security environment that is confronting Australia. The threat to Australians from espionage and foreign interference is higher than at any time in Australia's history. In this context, the threats posed are higher for new applicants who do not have hold a security clearance and are not existing Commonwealth employees. Additionally, such applicants may not yet have a sufficient understanding of their security obligations and may unwittingly or knowingly already be vulnerable to approaches from adversaries which they are less able to manage.

The Bill would therefore provide these persons with a right to seek independent review by a person appointed by the Attorney-General as an alternative to AAT review, where security risks can be more readily mitigated than in AAT proceedings. This review maintains independent oversight of ASIO's security clearance decisions and provides a further opportunity for ASIO to make a new security clearance decision for an affected person – but does not oblige ASIO to do so.

Existing security clearance holders and Commonwealth employees are not provided with a pathway to an independent reviewer because the security risks are not considered as high. Instead, these individuals have access to an external merits review process in the AAT, in which they could actively participate, that would result in findings that are binding on ASIO. This is similar to existing rights available to some individuals to seek AAT review of adverse and prejudicial security assessments under Part IV of the ASIO Act. The AAT is designed to review administrative decisions made by Government and is ideally placed to provide a rigorous and independent review that is appropriate having regard to the potential

impacts of adverse decisions on existing security clearance holders and Commonwealth employees.

In respect of whether potential conflict of interest could arise when the independent reviewer is required to determine whether to review a matter or not— the Bill enables the independent reviewer to decide whether to review a decision (proposed section 83EB(3)). The lack of a specific threshold in this provision was a deliberate approach to maximise the independent reviewer's ability to account for all factors they consider relevant in making such a decision, and to ensure the independent reviewer has flexibility to manage their caseload.

It is not expected that the independent reviewer's remuneration arrangements will materially affect a decision of whether to review a security clearance decision. The terms of engagement would govern the Independent Reviewer's conduct and include a framework for managing conflicts of interest. The terms of engagement would also govern termination. In the event of a breach of the terms of engagement, including any real or apparent interests that could improperly influence the Independent Reviewer's conduct, which have not been managed in accordance with the conflict of interest framework, the engagement could be terminated.

The Bill also provides that the independent reviewer must have appropriate skills or qualifications to perform the role, and the highest level of security clearance. These threshold requirements in the Bill are designed to ensure that the independent reviewer will not just be appropriately skilled or qualified, but also be a person of integrity. In particular, the standards required to hold the highest level of security clearance will ensure high levels of integrity.

In respect of why the Bill is silent in respect to the independent reviewer not providing information to any other unauthorised person when the Bill requires the independent reviewer to do all things necessary to ensure that any information provided to them is not disclosed to the affected person—the Bill provides at section 83EC(5)(a) that the Independent Reviewer must comply with any reasonable directions of the Director-General of Security in relation to the protection or handling of information provided to the Independent Reviewer under section 83EC. Therefore, the Director-General can, on a case by case basis, determine how information should be protected or handled under the Bill.

Australian Government
Australian Security Intelligence Organisation

Attachment A

ASIO
Securing Australia—protecting its people

Countering the insider threat

What the threat looks like

Insiders are current and former employees or contractors who have legitimate or indirect access to your workplace's people, information, techniques, activities, technology, assets or facilities.

Insiders may conduct activities that could harm your workplace, be detrimental to Australia's national security, undermine Australia's sovereignty and prosperity, or even pose a threat to life.

Unintentional insiders

inadvertently betray the trust placed in them.

Intentional insiders

deliberately betray the trust placed in them.

Both intentional and unintentional insiders may assist a third party, such as a foreign power or their proxy. They may willingly assist, be coerced to assist, be unknowingly exploited, or be unaware that their actions are harmful.

The most frequent type of insider activity involves the unauthorised disclosure of privileged information.

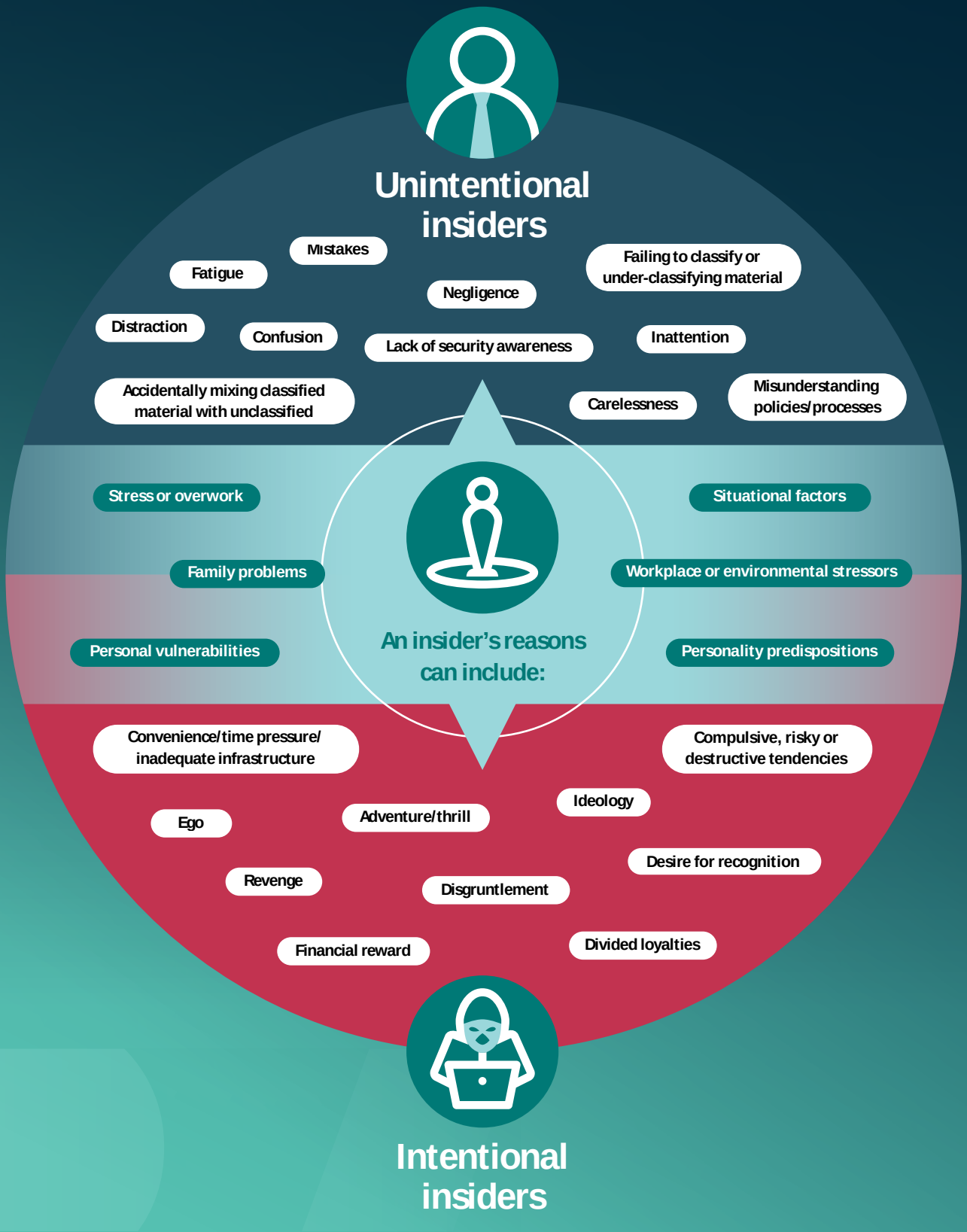
Examples of unintentional insider activity include:

- absent-mindedly clicking on email links that lead to malicious network compromise by a third party;
- misplacing a workplace-issued security pass, electronic device or sensitive document;
- being unknowingly exploited by a third-party, such as a foreign power, competitor, friend or associate;
- carelessly oversharing privileged information at a social gathering or in a public place; or
- mistakenly providing information to a colleague who doesn't have an appropriate security clearance or valid need to know.

Examples of intentional insiders include individuals who:

- publicly disclose classified or privileged information as an act of revenge; or
- share sensitive intellectual property with a third party—such as a foreign power—in exchange for payment or other personal benefit.

Insiders can have varied and often complex reasons for conducting harmful activities and may conduct those activities intentionally or unintentionally.



What you can do about it

Workplaces can harden themselves to the insider threat, and limit the damage if compromise occurs, by establishing a **counter insider threat program (CITP)**. A CITP is a set of measures to **manage the risk of**, and **deter**, **detect**, **respond to** and **recover from**, the insider threat.

ASIO recommends that your CITP focuses on six key areas:

1. **Conduct a risk assessment and develop a security plan**
2. **Establish governance, communications and relationships**
3. **Develop a robust security culture**
4. **Implement a personnel security framework**
5. **Implement physical and ICT detection and control measures**
6. **Establish assessment and response mechanisms**

Security is a shared responsibility

Work together; no single area or person can manage the threat alone.

Resources

ASIO has developed the *Counte**ring the insider threat: a security** manager's guide* to assist eligible security managers to understand the threat and develop a CITP. Visit www.asio.gov.au for more information.

The Protective Security Policy Framework—www.protectivesecurity.gov.au

The Australian Cyber Security Centre—www.cyber.gov.au

Report concerning behaviour

To report possible **espionage, foreign interference, sabotage, disclosure of national security information, or terrorist or security-related activities that seem suspicious, unusual or persistent**:

- if you work in an Australian Government organisation or hold a security clearance, contact your security team to complete a contact report; or
- if you work in private industry, report to your security team, the National Security Hotline on 1800 123 400 or to ASIO via the Notifiable Incidents, Threats or Reportable Observations (NITRO) portal—nitro.asio.gov.au.

To report a **cyber incident**, visit cyber.gov.au or call the Australian Cyber Security Hotline on 1300 CYBER1 (1300 292 371).

To report possible **criminal activity**, contact your local police or call Crime Stoppers on 1800 333 000.