23 January 2025

Oliver Smith
BY EMAIL: foi+request-12551-9c46d14d@righttoknow.org.au

In reply please quote:
FOI Request: FA 24/12/00616
File Number: FA24/12/00616

Dear Oliver Smith

Freedom of Information (FOI) request – Decision

On 11 December 2024, the Department of Home Affairs (the Department) received a request for access to document under the *Freedom of Information Act 1982* (the FOI Act).

The purpose of this letter is to provide you with a decision on your request for access under the FOI Act.

1 Scope of request

You have requested access to the following document:

> *Under the FOI Act, I seek a copy of the Ministerial Brief provided to the office of Home Affairs Minister Tony Burke on 3/9/24 with the PDR No. MS24-001634.*

2 Authority to make decision

I am an officer authorised under section 23 of the FOI Act to make decisions in respect of requests to access document or to amend or annotate records.

3 Relevant material

In reaching my decision I referred to the following:

- the terms of your request
- the document relevant to the request
- the FOI Act
- Guidelines published by the Office of the Information Commissioner under section 93A of the FOI Act (the FOI Guidelines)
- consultation responses from third parties consulted in accordance with the FOI Act
- advice from Departmental officers with responsibility for matters relating to the document to which you sought access

4 Document in scope of request

The Department has identified one document as falling within the scope of your request. This document was in the possession of the Department on 11 December 2024 when your request was received.

5 Decision

The decision in relation to the document in the possession of the Department which fall within the scope of your request is as follows:

- Exempt one document in full from disclosure

6 Reasons for Decision

My findings of fact and reasons for deciding that the exemption provision applies to that information are set out below.

6.1 Section 33 of the FOI Act – Documents affecting National Security, Defence or International Relations

Section 33(a)(i) of the FOI Act permits exemption of a document if disclosure of the document would, or could reasonably be expected to cause damage to the security of the Commonwealth.

For the reasons set out below, I consider that there are real and substantial grounds for expecting that the disclosure of the documents exempted under section 33(a)(i) would cause damage to the security of the Commonwealth.

Security

'Security' is a concept with a fluctuating content which can depend upon the circumstances as they exist from time to time.[1] 'Security of the Commonwealth' is defined in section 4(5) of the FOI Act as follows

> *(5) Without limiting the generality of the expression security of the Commonwealth, that expression shall be taken to extend to:*
>
> *(a) matters relating to the detection, prevention or suppression of activities, whether within Australia or outside Australia, subversive of, or hostile to, the interests of the Commonwealth or of any country allied or associated with the Commonwealth; and …*

I also consider that the definition of 'security' in the *Australian Security and Intelligence Organisation Act 1979* (the ASIO Act) is relevant. This view is in accordance with the guidance provided by *Staats and National Archives of Australia,*[2] in which Deputy President Forgie found that it would be 'consistent with the scheme of regulation established by Parliament to interpret the word "security" in both the Archives Act and the FOI Act in a way that mirrors its definition in the ASIO Act'.

---

[1] *Church of Scientology v Woodward* (1982) 154 CLR 25 at [19].
[2] Staats and National Archives of Australia [2010] AATA 531 (16 July 2010) (austlii.edu.au), at [99]

The ASIO Act defines 'security' as:

(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.

In recent years, the Australian Government has made great advances in bringing its business online. The benefits of government information and communications technology (ICT) systems and services becoming increasingly connected will continue as the government makes the most of new technologies. However, this new, connected way of doing business also creates opportunities for adversaries to gain an advantage by exploiting these technologies to access information of national importance. As our intrusion detection, response, mitigation and threat assessment capabilities continue to improve, so too do the skills of cyber threat actors. This requires us to be vigilant, flexible and proactive in our approach to cyber and information security. A strong security posture requires ongoing vigilance and resources. By continually hardening our defences, we have a greater chance of protecting the information entrusted to us. The Australian Government Information Security Manual (ISM) comprises three complementary documents designed to provide greater accessibility and understanding at all levels of government. This Executive Companion details the cyber security threat and introduces considerations for those most senior in an organisation in mitigating the risks presented by this threat environment.

The security of sensitive government and commercial information, the security of our digital infrastructure, and public and international confidence in Australia as a safe place to do business online are critical to our future. Because any Internet–connected device or computer system is highly susceptible to malicious cyber activity, our dependence on ICT also brings greater exposure to threats. The threat is not limited to classified systems and information

The Department has developed a Protective Security Policy Framework (PSPF), which includes information security management policies.

The PSPF ensures that:

- all official information is safeguarded to ensure its confidentiality, integrity, and availability by applying safeguards so that:
- only authorised people, using approved processes, access information
- information is only used for its official purpose, retains its content integrity, and is available to satisfy operational requirements
- information is classified and labelled as required.
- all information created, stored, processed, or transmitted in or over government information and communication technology (ICT) systems is properly managed and protected throughout all phases of a system's life cycle, in accordance with the protocols and guidelines set out in the PSPF, which includes the Australian Government Information Security Manual, produced by the Australian Signals Directorate.

Successfully protecting Australian networks from an increasingly sophisticated and persistent cyber threat requires strong collaboration.

For a document to be exempt under s 33(a)(i), I must be satisfied that, on the balance of probabilities, disclosure would, or could reasonably be expected to, cause damage to the security of the Commonwealth.

As such I have decided that the document(s) is exempt from disclosure under section 33(a)(i) of the FOI Act.

7 Legislation

A copy of the FOI Act is available at https://www.legislation.gov.au/Series/C2004A02562. If you are unable to access the legislation through this website, please contact our office for a copy.

8 Your review rights

If you disagree with this decision, you have the right to apply for either an internal review or an Information Commissioner review of the decision.

Internal review

If you want the Department to review this decision, you must make your internal review request within 30 days of being notified of this decision.

When making your internal review request, please provide the Department with the reasons why you consider this decision should be changed.

You can send your internal review request to:

Email: foi.reviews@homeaffairs.gov.au

Or

Postal mail:
Freedom of Information
Department of Home Affairs
GPO Box 241 MELBOURNE VIC 3001

The internal review will be carried out by an officer who is more senior than the original decision maker. The Department must make its decision on the review within 30 days of receiving your request for internal review.

Information Commissioner review

If you want the Australian Information Commissioner to review this decision, you must make your request to the Office of the Australian Information Commissioner (OAIC) within 60 days of being notified of this decision.

You can apply for an Information Commissioner review using the Information Commissioner review application form on the OAIC website.

You can find more information about Information Commissioner reviews on the OAIC website.

9 Making a complaint

You may make a complaint to the Australian Information Commissioner if you have concerns about how the Department has handled your request under the FOI Act. This is a separate process to the process of requesting a review of the decision as indicated above.

You can make an FOI complaint to the Office of the Australian Information Commissioner (OAIC) at: FOI Complaint Form on the OAIC website.

10 Contacting the FOI Section

Should you wish to discuss this decision, please do not hesitate to contact the FOI Section at foi@homeaffairs.gov.au.

Yours Sincerely

(Electronically signed)

Tony
Position number: 6170573
Authorised Decision Maker
Department of Home Affairs