

OFFICIAL: ~~Sensitive~~

Australian Government
Department of Home Affairs

Submission

For decision
 PDMS Ref. Number: MS25-001221
 Date of Clearance: 03/02/2026

To Minister for Home Affairs, Minister for Immigration and Citizenship,
 Minister for Cyber Security

Subject Minister seeking the Prime Minister's approval for Cyber Incident
 Review Board appointments

Timing For consideration by 23 February 2026 in order to appoint the Chair and standing
 members to the Cyber Incident Review Board.

Recommendations

That you:

1. **sign** the attached letter to the Prime Minister, the Hon Anthony Albanese MP, seeking his agreement to appoint your preferred candidates to the Cyber Incident Review Board (the Board) Attachment A; and
2. **approve** the Media and Communications Plan for the announcement of the appointment of the Board Attachment B.

signed / not signedapproved / not approved

Minister for Home Affairs, Minister for Immigration and
 Citizenship, Minister for Cyber Security

Signature.....

Date.....182/2026

OFFICIAL: ~~Sensitive~~

Minister's Comments

*It would appear these
recs only involve people
from NSW, ACT, & Vic. This
is not appropriate for a national
board.*

Key Issues

1. This submission seeks your agreement to write to the Prime Minister to approve the appointment of your preferred candidates to the Chair and standing members of the Board Attachment A.
 - As appointments to the Board are classified as significant appointments, the approval of the Prime Minister is required.
2. Your preferred candidates have indicated their availability for appointment to the Board and s. 22(1)(a)(ii) has agreed to be appointed to the position of Chair;

Proposed candidate for Chair

- s. 22(1)(a)(ii)

Proposed candidates for standing members

s. 22(1)(a)(ii)

3. This submission also provides attachments that must accompany your letter to the Prime Minister. These include a curriculum vitae and private interest declaration for each candidate. Attachment C.
 - The Department of Home Affairs (the Department) has undertaken due diligence checks on the information provided by the candidates. There are no conflicts of interest or adverse findings which would compromise a candidate's ability to perform their duties as a Board member. The Department has prepared a candidate due diligence record for your information Attachment D.

Next Steps

4. Following approval from the Prime Minister, the Department will provide you with written instruments to make these appointments.

OFFICIAL: Sensitive

5. In consultation with your office, the Department has prepared a Media and Communications Plan **Attachment B**. We will continue to work with your office on the timing of the announcement.
6. Once appointed, the Board will establish its internal governance and processes in line with the *Cyber Security Act 2024* (the Act). This will include identifying suitable individuals for appointment to the Expert Panel.
7. Following their appointment, the Board may consider referrals and conduct reviews.

Background

8. Following the approval by the Prime Minister, granted on 2 September 2025, (MC25-11707 refers), the Department published an expression of interest (EOI) for suitable candidates for the Board on the Home Affairs website.
9. The Department received 185 applications. All applications underwent an initial review by senior members of the Department to confirm eligibility against the criteria in section 13 of the Cyber Security (Cyber Incident Review Board) Rules 2025.
10. On 15 October 2025, the Department provided you with a submission containing a list of eligible candidates received from the EOI exercise (MS25-003313 refers).

Consultation - Internal/External

11. **External:** The Department of Prime Minister and Cabinet was consulted on the appointment information provided by the selected candidates.
12. **Internal:** The Department's media and communications team was consulted on the Media and Communications Plan.

Risks and Sensitivities

13. The legislation to establish the Board took effect on 30 May 2025 and there is growing interest in when the Board will be established. The Department will continue to manage this interest via regular updates to its website and ongoing consultation with stakeholders.
14. The EOI was conducted under an exemption from the Government's Merit and Transparency Policy (the Policy) from the Prime Minister which may give rise to concerns that the appointments were not made based on merit. The Department has implemented measures to replicate the usual processes undertaken through the Policy, including an independent, transparent, and merit-based review of candidates.
15. Not all candidates currently hold an Australian security clearance or equivalent clearance that would be recognised in Australia. If selected, the Department will sponsor and work with those candidates to obtain their security clearance.
 - Individuals appointed without holding a clearance will still be able to assist the governance of the Board and elements of a review which are classified below Protected.

Financial/systems/legal/deregulation/media implications

16. There are no financial, systems, legal or deregulation implications.

OFFICIAL: Sensitive

OFFICIAL: Sensitive

Attachments

- Attachment A** Draft letter to the Prime Minister
- Attachment B** Communications and Media Plan
- Attachment C** Board member candidate appointment package
- Attachment D** Candidate due diligence record

Authorising Officer

Cleared by:

Ciara Spencer
Deputy Secretary
Law Enforcement & Domestic Security Group

Date: 03/02/2026

Mob: [REDACTED] 22(1)(a)(ii)

Contact Officer: Ash Bell, A/g First Assistant Secretary, CFI, Cyber and Technology Division, [REDACTED] 22(1)(a)(ii)

CC Head of National Security
 DS Chief Operating Officer
 DS Executive
 DS Legal
 FAS CFICT
 FAS Executive Coordination

OFFICIAL: Sensitive



The Hon Tony Burke MP
Minister for Home Affairs
Minister for Immigration and Citizenship
Minister for Cyber Security
Minister for the Arts
Leader of the House

Ref No: MS25-001221

The Hon Anthony Albanese MP
Prime Minister
Parliament House
CANBERRA ACT 2600

Dear Prime Minister

I am writing to seek your agreement for me as the Minister for Cyber Security, to appoint my selected nominees for the Cyber Incident Review Board (the Board) under the *Cyber Security Act 2024* (the Act). In accordance with the Act, I may appoint a Chair and up to 6 standing members to the Board.

In September last year, you granted an exemption from the Australian Public Service Commission (APSC) Merit and Transparency Policy for the appointment of the Board, ([MS25-002555](#) refers). The Department of Home Affairs then conducted a 4-week expression of interest (EOI) process and provided me with a list of suitable candidates for consideration.

Due care has been taken at each stage of the EOI recruitment to ensure that the process for the Board appointments aligns with the principles of the Merit and Transparency Policy:

- The EOI was publicised broadly through the 2500-member Trusted Information Sharing Network and amplified across the Department's relevant social media profiles.
- The Department received in total, 185 eligible submissions which were assessed for suitability against the eligibility criteria in section 13 of the *Cyber Security (Cyber Incident Review Board) Rules 2025* and using an approved skills matrix.

In making my determination I have considered all 185 applicants and given due consideration not only to their individual merits, but also to ensuring the representation of women, culturally and linguistically diverse persons, and geographic position; to reflect the Government's commitment to equity and diversity in making senior government appointments.

I have identified the following individuals for appointment to the Board. Their curricula vitae and private interest declarations are enclosed for your consideration.

Proposed candidate for Chair

➤ s. 22(1)(a)(ii)

Proposed standing members

s. 22(1)(a)(ii)

The Department has conducted rigorous due diligence and background checks to ensure the selected candidates had the character and qualities to represent the Board. No issues or concerns have been identified with the proposed nominees that may give rise to a real or perceived conflict of interest that would cast doubt on the integrity or independence of the Board.

Following your agreement with the proposed appointees, I will write formally to the candidates with a letter of offer and proceed with the appointments. The Department will liaise with my office and the Department of the Prime Minister and Cabinet to deliver the media and communications for the public announcement of the Board.

Yours sincerely

Tony Burke

/ / 2026



OFFICIAL: ~~Sensitive~~

Cyber Incident Review Board Appointments: Communication Plan

Purpose

This Communications Plan outlines the approach and activities to be undertaken to announce the appointment of the Chair and standing members of the Cyber Incident Review Board (the Board).

Communication objectives

Communication activities will seek to:

- Raise awareness of the appointment to the Board, and the commencement of its functions
- Inform Australian businesses, industry groups, international partners and government stakeholders of the establishment of the Board
- Seek industry support and buy-in for the Board
- Attract prospective candidates to participate in the Expert Panel; and
- Promote the role of the Board to uplift Australia's cyber resilience

Target audiences

- Australian businesses
- Owners and operators of critical infrastructure
- Civil society and academia
- Peak bodies or industry specialists, and
- Commonwealth, State or Territory governments who have a collective responsibility for cyber security and critical infrastructure security

Key Messages

The Minister for Home Affairs (the Minister), has appointed the Chair and 6 standing members to establish the Cyber Incident Review Board. These appointments reflect the high calibre of Australia's cyber security expertise and leadership.

OFFICIAL: ~~Sensitive~~

The Following candidates have been appointed:

Proposed candidate for Chair

s. 22(1)(a)(ii)

Proposed candidates for standing members

s. 22(1)(a)(ii)

The *Cyber Security Act 2024* (the Act) established the Cyber Incident Review Board as an independent statutory advisory body to conduct no-fault, post-incident reviews of significant cyber security incidents in Australia.

Recent high-profile and high-impact cyber security incidents highlight the need for industry and Government to do more to effectively review and learn lessons from cyber security incidents and to prepare contingencies for future attacks.

Australia needs an independent mechanism responsible for undertaking post-incident reviews of significant cyber security incidents, and the effectiveness of government and industry response.

The Cyber Incident Review Board will uplift Australia's collective cyber security by boosting our ability to hone incident preparation and response.

It's important that we understand the vulnerabilities that led to the attack when a major incident occurs and to share lessons learned with industry, government and the public to improve future cyber readiness.

The Board has broad independence in deciding which cyber incidents it will review and how the Board will operate. The Board will work cooperatively with industry to enhance Australia's collective cyber resilience.

Lessons learned from reviews will be shared with the business community and the wider public. The Board will provide actionable recommendations to government and industry in order to prevent, detect, respond to, or minimise the impact of cyber security incidents of a similar nature in the future.

Background

Establishment under the Act

- The Act established the Board as an independent statutory advisory body with a remit to conduct no-fault, post-incident reviews of significant cyber security incidents in Australia.
- The Board will provide actionable recommendations to government and industry in order to prevent, detect, respond to, or minimise the impact of cyber security incidents of a similar nature in the future.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

- The Board is a key component of the Australian Government's 2023-2030 Australian Cyber Security Strategy vision for building resilient and cyber future ready communities, strong businesses and a secure Australian economy.
- The Board will not act as an investigatory body that apportions blame or determines the liability of any entity in relation to a cyber security incident. The Board will have independence and enable Australia to learn from cyber security incidents and continuously uplift our national resilience.

Composition of the Board

- The Minister will appoint a Chair and up to 6 standing members from both the public and private sectors. The Board will be composed of a cross section of the Australian community and business sector; diverse in professional experience, gender, cultural background and age.
- The appointed Chair and standing members will be updated in **Attachment A**, pending the approval of the Minister and the Prime Minister (these are considered significant appointments).
- An Expert Panel will support the Board, comprised of relevantly experienced individuals. These individuals will form a large pool of pre-cleared experts that the Board can appoint to a review panel to assist with the conduct of a review, providing specialist expertise.
- The Expert Panel will be established once the Board is in place, as the Board sees fit. Individuals may register their interest in applying to join the Expert Panel by emailing CIRB.Enquiries@homeaffairs.gov.au.

Eligibility

- The Cyber Security (Cyber Incident Review Board) Rules 2025, established eligibility criteria for the Board, for example qualifications or experience in the field of cyber security and incident management or crisis response.
- Standing members and the Expert Panel will have a requirement to hold or be eligible to obtain an Australian security clearance or an equivalent security clearance recognised by the Commonwealth that allows the person access to information that has a security classification of at least secret.
- The Board and Expert Panel are required to disclose all interests they may have, pecuniary or otherwise, in relation to the Board or its equities and may be required to recuse themselves from involvement in matters undertaken by the Board in which they have an interest.

Remuneration

- Board members will be remunerated through a daily fee model, as established through determination by the Remuneration Tribunal.
- Expert Panel members appointed to a review panel for a review are eligible to be paid the remuneration and allowances determined by the Chair of the Board by legislative instrument. The amount of remuneration will be informed by what other individuals received performing similar or equivalent functions within Government and industry.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

Activity timeline

Phase	Description	Audience	Timing	Channel
2026				
Appointment of the Board	1. Media Release from MHA announcing appointment of Chair and standing members	- Australian businesses - Peak bodies or industry specialists - Prospective Expert Panel members	Release by MO dependant on MHA appointment and letters sent to Chair and standing members	Home Affairs website
	2. Supporting MHA talking points			
	3. Website update with biographies or blurbs of Board appointees	As above	Simultaneous to Media Release	Home Affairs website
Promoting Chair and Board members	4. Social media tiles introducing the Board	As above	Pending Board members' approval	Home Affairs social media, shared by CIPP

Released by Department of Home Affairs
under the Freedom of Information Act 1982

Attachment A: Chair and standing member biographies

To be confirmed with nominees, subject to approvals

Released by Department of Home Affairs
under the Freedom of Information Act 1982

	Conflict of Interest (Col)	Media and Communications Checks			Financial Checks							
Candidate Name	PID identifies any conflict of interest(s), either actual, perceived, or potential.	Social media check	Media & Press coverage including associated companies, businesses.	Review for negative public commentary	Bankruptcy Register Search	ASIC Register comprehensive search to affirm banned or disqualified status and other related business or person searches.	Affiliations with industry or previous companies that may carry any perceived or actual conflict of interest risk.	Civil or criminal proceedings or enforcement action, in relation to the management of an entity, or commercial or professional activities	Substantial involvement in the management of a business or company which has failed	Perpetrated or participated in negligent, deceitful, or otherwise discreditable business or professional practices	Civil or criminal proceedings or enforcement action, which adversely reflects on the candidate's competence, diligence, judgement, honesty or integrity	Involvement with management of a business or company which has failed

s. 22(1)(a)(ii)



Australian Government
Department of Home Affairs

Submission

For decision

PDMS Ref. Number: MS26-000559

Date of Clearance: 18/03/2026

To Minister for Home Affairs, Minister for Immigration and Citizenship,
Minister for Cyber Security

Subject Minister seeking the Prime Minister's approval for Cyber Incident
Review Board appointments

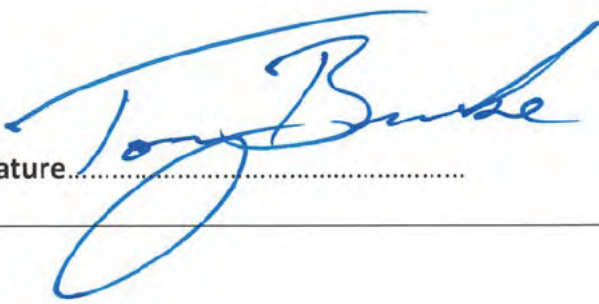
Timing For consideration by 30 March 2026, as agreed by the Office, in order to appoint
Chair and standing members to the Cyber Incident Review Board.

Recommendations

That you:

1. **sign** the attached letter to the Prime Minister,
the Hon Anthony Albanese MP, seeking agreement to
appoint your preferred candidates to the Cyber Incident
Review Board; and signed / not signed
2. **approve** the Media and Communications Plan for
announcement of the appointment of the Cyber Incident
Review Board (**Attachment 8**). approved / not approved

Minister for Home Affairs, Minister for Immigration and
Citizenship, Minister for Cyber Security

Signature.....


Date: 20/3/2026

Released by Department of Home Affairs
under the Freedom of Information Act 1982

Minister's Comments

Key Issues

1. This submission recommends you write to the Prime Minister, the Hon Anthony Albanese MP, to approve the appointment of your preferred candidates as Chair and standing members of the Cyber Incident Review Board (**Attachment A**).
 - As appointments to the Cyber Incident Review Board are classified as significant appointments, the approval of the Prime Minister is required.
2. Your preferred candidates have indicated their availability for appointment to the Cyber Incident Review Board, and s. 22(1)(a)(ii) has agreed to be appointed to the position of Chair:

Proposed candidate for Chair

- s. 22(1)(a)(ii)

Proposed candidates for standing members

s. 22(1)(a)(ii)

3. This submission provides attachments that must accompany your letter to the Prime Minister. These include a curriculum vitae and private interest declaration for each candidate (**Attachment C**).
 - The Department of Home Affairs (the Department) has undertaken due diligence checks on the information provided by the candidates. There are no conflicts of interest or adverse findings which would compromise a candidate's ability to perform their duties as a board member. The Department has prepared a candidate due diligence record for your information (**Attachment D**).
4. This submission also seeks your approval of the Media and Communications Plan for announcement of the appointment of the Cyber Incident Review Board (**Attachment B**).

Next Steps

5. Following approval from the Prime Minister, the Department will provide you with written instruments to make these appointments.

6. In consultation with your office, the Department has prepared a Media and Communications Plan (**Attachment B**). The Department will continue to work with your office on the timing of the announcement.
7. Once appointed, the Cyber Incident Review Board will establish its internal governance and processes in line with the *Cyber Security Act 2024* (Cth). This will include identifying suitable individuals for appointment to the Expert Panel.

Background

8. Following approval by the Prime Minister, granted on 2 September 2025, (MC25-11707 refers), the Department published a call for expressions of interest for suitable candidates for the Cyber Incident Review Board on the Home Affairs website.
9. The Department received 185 applications. All applications underwent an initial review by senior members of the Department to confirm eligibility against the criteria in section 13 of the *Cyber Security (Cyber Incident Review Board) Rules 2025*.
10. On 20 November 2025, you nominated your preferred candidates from a list of eligible candidates provided by the Department. This list was compiled from applications received in the expression of interest process (MC25-003313 refers).
11. On 3 February 2026, the Department sought your agreement to a draft letter to the Prime Minister, seeking his agreement to appoint your preferred candidates to the Cyber Incident Review Board (MS25-001221 refers).
 - On 18 February 2026, you advised that broader state and territory representation – beyond New South Wales, Victoria and the Australian Capital Territory – is more appropriate for a national board (MS25-001221 refers).
12. On 19 February 2026, the Department provided to your office details of eligible candidates from Queensland, South Australia and Western Australia. The list of proposed candidates for standing members (paragraph 2 above refers) has been updated in line with agreement of your office.
13. Following the Prime Minister's agreement to your proposed appointments, the Department will advise the 2 candidates no longer being considered for a position on the Cyber Incident Review Board of the final outcome of the selection process. The 2 candidates are:

s. 22(1)(a)(ii)

Consultation – Internal/External

14. **External:** The Department of the Prime Minister and Cabinet was consulted on the appointment information provided by the selected candidates.
15. **Internal:** The Department's media and communications team was consulted on the Media and Communications Plan.

Risks and Sensitivities

16. The legislation to establish the Cyber Incident Review Board took effect on 30 May 2025, and there is growing interest in when the board will be established. The Department will continue to manage this interest via regular updates to its website and ongoing consultation with stakeholders.
17. The expression of interest exercise was conducted under an exemption from the Government's Merit and Transparency Policy, granted by the Prime Minister, which may give rise to concerns that the appointments were not made based on merit. The Department has implemented measures to replicate the usual processes undertaken through the policy, including an independent, transparent and merit-based review of candidates.
18. Not all proposed candidates currently hold an Australian security clearance or equivalent clearance that would be recognised in Australia. If selected, the Department will sponsor and work with those candidates to obtain an appropriate security clearance.
- Individuals appointed without holding a clearance will still be able to assist with the governance of the Cyber Incident Review Board and elements of a cyber incident review which are classified below PROTECTED.

Financial/systems/legal/deregulation/media implications

19. There are no financial, systems, legal or deregulation implications.

Attachments

Attachment A Draft letter to the Prime Minister

Attachment B Communications and Media Plan

Attachment C Candidate CV and PID Package

Attachment D Due Diligence Background Checks

Authorising Officer
Cleared by:
Ciara Spencer Deputy Secretary Law Enforcement & Domestic Security Group
Date: 18/03/2026
Mob: s. 22(1)(a)(ii)

Contact Officer: Ash Bell, Assistant Secretary, Cyber Policy and Programs, Ph: s. 22(1)(a)(ii)

CC Head of National Security
DS Chief Operating Officer
DS Executive
DS Legal
FAS CFICT
FAS Executive Coordination

Released by Department of Home Affairs
under the Freedom of Information Act 1982



The Hon Tony Burke MP
Minister for Home Affairs
Minister for Immigration and Citizenship
Minister for Cyber Security
Minister for the Arts
Leader of the House

Ref No: MS26-000559

The Hon Anthony Albanese MP
Prime Minister
Parliament House
CANBERRA ACT 2600

Dear Prime Minister

I am writing to seek your agreement for me, as the Minister for Cyber Security, to appoint my selected nominees to the Cyber Incident Review Board (the Board) under the *Cyber Security Act 2024* (Cth) (the Act). In accordance with the Act, I may appoint a Chair and up to 6 standing members to the Board.

In September last year, you granted an exemption from the Australian Public Service Commission (APSC) Merit and Transparency Policy for the appointment of the Board (MS25-002555 refers). The Department of Home Affairs (the Department) then conducted a 4-week expression of interest (EOI) process and provided me with a list of suitable candidates for consideration.

Due care has been taken at each stage of the EOI recruitment to ensure that the process for the Board appointments aligns with the principles of the Merit and Transparency Policy:

- The EOI was publicised broadly through the 2500-member Trusted Information Sharing Network and amplified across the Department's relevant social media profiles.
- The Department received 185 eligible submissions in total, which were assessed for suitability against the eligibility criteria in section 13 of the *Cyber Security (Cyber Incident Review Board) Rules 2025* and using an approved skills matrix.

In making my determination, I have considered all 185 applicants and given due consideration not only to their individual merits, but also to ensuring the representation of women, culturally and linguistically diverse persons, and geographic position; to reflect the Government's commitment to equity and diversity in making senior government appointments.

I have identified the following individuals for appointment to the Board. Their curricula vitae and private interest declarations are enclosed for your consideration.

Proposed Chair

- s. 22(1)(a)(ii)

Proposed standing members

s. 22(1)(a)(ii)

The Department has conducted rigorous due diligence and background checks to ensure the selected candidates have the character and qualities to represent the Board. No issues or concerns have been identified with the proposed nominees that may give rise to a real or perceived conflict of interest that would cast doubt on the integrity or independence of the Board.

Following your agreement with the proposed appointees, I will write formally to the candidates with a letter of offer and proceed with the appointments. The Department will liaise with my office and the Department of the Prime Minister and Cabinet to deliver the media and communications for public announcement of the Board.

Yours sincerely


 Tony Burke
 20 / 3 / 2026



The Hon Tony Burke MP
Minister for Home Affairs
Minister for Immigration and Citizenship
Minister for Cyber Security
Minister for the Arts
Leader of the House

Ref No: MS26-000559

The Hon Anthony Albanese MP
Prime Minister
Parliament House
CANBERRA ACT 2600

Dear Prime Minister

I am writing to seek your agreement for me, as the Minister for Cyber Security, to appoint my selected nominees to the Cyber Incident Review Board (the Board) under the *Cyber Security Act 2024* (Cth) (the Act). In accordance with the Act, I may appoint a Chair and up to 6 standing members to the Board.

In September last year, you granted an exemption from the Australian Public Service Commission (APSC) Merit and Transparency Policy for the appointment of the Board (MS25-002555 refers). The Department of Home Affairs (the Department) then conducted a 4-week expression of interest (EOI) process and provided me with a list of suitable candidates for consideration.

Due care has been taken at each stage of the EOI recruitment to ensure that the process for the Board appointments aligns with the principles of the Merit and Transparency Policy:

- The EOI was publicised broadly through the 2500-member Trusted Information Sharing Network and amplified across the Department's relevant social media profiles.
- The Department received 185 eligible submissions in total, which were assessed for suitability against the eligibility criteria in section 13 of the Cyber Security (Cyber Incident Review Board) Rules 2025 and using an approved skills matrix.

In making my determination, I have considered all 185 applicants and given due consideration not only to their individual merits, but also to ensuring the representation of women, culturally and linguistically diverse persons, and geographic position; to reflect the Government's commitment to equity and diversity in making senior government appointments.

I have identified the following individuals for appointment to the Board. Their curricula vitae and private interest declarations are enclosed for your consideration.

Proposed Chair

s. 22(1)(a)(ii)

Proposed standing members

s. 22(1)(a)(ii)

The Department has conducted rigorous due diligence and background checks to ensure the selected candidates have the character and qualities to represent the Board. No issues or concerns have been identified with the proposed nominees that may give rise to a real or perceived conflict of interest that would cast doubt on the integrity or independence of the Board.

Following your agreement with the proposed appointees, I will write formally to the candidates with a letter of offer and proceed with the appointments. The Department will liaise with my office and the Department of the Prime Minister and Cabinet to deliver the media and communications for public announcement of the Board.

Yours sincerely

Tony Burke

/ / 2026

OFFICIAL: ~~Sensitive~~

Australian Government
Department of Home Affairs

Submission

For decision

PDMS Ref. Number: MS25-003313

Date of Clearance: 15/10/2025

To Minister for Home Affairs, Minister for Immigration and Citizenship,
 Minister for Cyber Security

Subject Cyber Incident Review Board Appointments

Timing For consideration by 31 October 2025 in order to support the appointment of the
 Cyber Incident Review Board.

Recommendations

That you:

1. **nominate** your preferred candidate for the Cyber Incident Review Board Chair from the Expression of Interest Response Document (**Attachment A**) for the Department of Home Affairs to commence the appointment process for the Board; nominate / please discuss
2. **nominate** up to six preferred candidates for the Board standing members from the Expression of Interest Response Document (**Attachment A**); nominate / please discuss
- AND
3. **agree** to appoint both the Chair and standing members for four-year terms. agree / please discuss

Minister for Home Affairs, Minister for Immigration and
 Citizenship, Minister for Cyber Security

Signature.....

Date...../...../2025

2011

OFFICIAL: ~~Sensitive~~

	Minister's Comments

Key Issues

1. Following the approval by the Prime Minister, the Hon Anthony Albanese MP, granted on 2 September 2025, (MC25-11707 refers), the Department of Home Affairs (the Department) published an expression of interest (EOI) for suitable candidates for the Board on the Home Affairs website.
 - The Department received 185 applications. Applications have undergone an initial review by senior members of the Department to confirm eligibility against the criteria in section 13 of the Cyber Security (Cyber Incident Review Board) Rules 2025 (the Rules) and the CIRB Skills Matrix ([Attachment B](#)).
2. This submission seeks your selection of one candidate for the Chair of the Cyber Incident Review Board (the Board) from the list of candidates prepared by the Department ([Attachment A](#)).
3. This submission also seeks your selection of up to 6 preferred candidates for appointment as standing members of the Board ([Attachment A](#)).
 - The *Cyber Security Act 2024* provides that you may appoint a Chair and between 2 to 6 standing members to the Board.
 - The Department recommends that initially you establish the Board by appointing a Chair and 5 standing members. This provides flexibility to add an additional standing member once the Board is operational.
 - The Board will be remunerated as part-time office holders at the rate determined by the Remuneration Tribunal (MS25-000396 refers).
4. The candidates' pitch and curriculum vitae have been provided separately to your office in a zip file.

Next Steps

5. Following your selection of preferred candidates, the Department will contact the identified candidates to confirm their availability and seek additional information from them, including conflict of interest declarations, in accordance with the Cabinet Handbook guidelines.
6. The Department will also conduct a formal review of each candidate to assess the existence of any adverse information such as media, political affiliations or financial implications that may impact their eligibility for a Board position.

7. Upon completion of this process and as these are classified as significant appointment under the Cabinet Handbook, the Department will prepare a further Ministerial Submission for you to write to the Prime Minister seeking his approval to make the appointments.
 - The Submission will also include a proposed communications plan for announcing the Board's establishment.
8. Once the Prime Minister has agreed, we will provide you with a further briefing with letters to each of the candidates for you to formally appoint them.

Background

9. Part 5 of the *Cyber Security Act 2024* establishes the Board as an independent statutory advisory body with a remit to conduct no-fault, post-incident reviews of significant cyber security incidents in Australia.
10. The Board will undertake reviews into cyber security incidents which have, or have the potential, to seriously prejudice Australia's social and economic prosperity or the national security and defence of Australia. Recommendations provided by the Board will be shared with the business community and the wider public. Insights will feed into our national threat intelligence, sharing and blocking networks to improve our national cyber resilience.
11. An Expert Panel of industry leaders from across a range of sectors will assist the Board in the conduct of reviews according to their area of expertise. This will ensure the Board has the right mix of skills, expertise and experience available to conduct an effective review of an incident or series of incidents.
 - Once it is established, the Board will form the Expert Panel.

Consultation - Internal/External

12. The Department of Prime Minister and Cabinet were consulted on the candidates. The Australian Public Service Commission (APSC) was consulted on policy and processes.

Risks and Sensitivities

13. The legislation to establish the Board took effect on 30 May 2025 and there is growing interest in when the Board will be established. The Department will continue to manage this interest via regular updates to its website and ongoing consultation with stakeholders.
14. Some candidates advised that they do not currently hold an Australian security clearance or equivalent clearance that would be recognised in Australia. If selected, the Department will sponsor and work with candidates to obtain their security clearance.
15. There may be concerns raised regarding the composition of the Board and whether it represents a diverse cross-section of the Australian community. The Department applies the Government APS diversity and inclusive strategic frameworks within the selection process and utilises the skills matrix to ensure a diverse selection across the candidate list.

OFFICIAL: Sensitive

16. As the EOI was conducted under an exemption from the Government's Merit and Transparency Policy (the Policy) from the Prime Minister, there may be additional scrutiny or comments regarding appointees.

- The Department has implemented measures to replicate the usual processes undertaken through the Policy, including an independent, transparent and merit-based review of candidates.

17. If a cyber incident occurs before the Board is established, authorised entities may still refer the incident to the Board for review at a later date.

Financial implications

18. There are no financial, systems, legal or deregulation implications.

19. Media and Communication Branch have been consulted on the development of Department and Minister's Office web and socials communications for the EOI process.

Attachments

Attachment A Expression of Interest Response Document

Attachment B Cyber Incident Review Board Skills Matrix

Authorising Officer
Ciara Spencer Deputy Secretary Law Enforcement & Domestic Security Group
Mob: s. 22(1)(a)(ii)
Date: 15/10/2025

Contact Officer: Ashley Bell, Assistant Secretary, Cyber Policy and Programs s. 22(1)(a)(ii)

CC DS Chief Operating Officer
DS Executive
DS Legal
FAS Executive Coordination
FAS Counter Foreign Interference, Cyber and Technology

OFFICIAL: Sensitive

Cyber Incident Review Board																			
Applicant					Job Title		Location and Diversity			Eligibility Criteria									
											To be eligible for the Board, candidates must be able to obtain a NV1 level security clearance and meet at least one of the other eligibility criteria								
											MUST MEET	MUST MEET at least one of the the following criteria							
No.	Last Name	First Name	Title	Position Applied to	Position held	Company	State and Territory	Gender	Aboriginal or Torres Strait Islander Heritage	CALD	Applicant has or is eligible to hold an Australian Security Clearance (or recognised equivalent)	Legal Qualification and Experience	Professional experience in Cyber or Information Security	Significant experience in audit, assurance or review processes, public administration or financial or prudential regulation	Significant experience in Incident management or crisis response	Significant experience in a critical infrastructure sector	Educational qualification in cyber security or information security	Academic qualifications or knowledge in a relevant field	Commonwealth, State or Territory government position at a senior level
Australian Capital Territory																			
1	s. 22(1)(a)(ii)																		
2	s. 22(1)(a)(ii)																		
3																			
4																			
5																			
6																			

Cyber Incident Review Board											Eligibility Criteria								
Applicant				Job Title		Location and Diversity			To be eligible for the Board, candidates must be able to obtain a IV1 level security clearance and meet at least one of the other eligibility criteria.										
No.	Last Name	First Name	Title	Position Applied to	Position Held	Company	State and Territory	Gender	Aboriginal or Torres Strait Islander Heritage	CALD	MUST MEET	MUST MEET at least one of the the following criteria							
											Applicant has or is eligible to hold an Australian Security Clearance (or recognised equivalent)	Legal Qualification and Experience	Professional experience in Cyber or Information Security	Significant experience in audit, assurance or review processes, public administration or financial or prudential regulation	Significant experience in incident management or crisis response	Significant experience in a critical infrastructure sector	Educational qualification in cyber security or information security	Academic qualifications or knowledge in a relevant field	Commonwealth, State or Territory government position at a senior level
7	s. 22(1)(a)(ii)																		
8																			
9	s. 22(1)																		
	Chair																		
10	s. 22(1)(a)(ii)																		
11																			
12																			
13																			

Cyber Incident Review Board																	
Applicant				Job Title		Location and Diversity				Eligibility Criteria							
										To be eligible for the Board, candidates must be able to obtain a NV1 level security clearance and meet at least one of the other eligibility criteria							
No.	Last Name	First Name	Title	Position Applied to	Position held	Company	State and Territory	Gender	Aboriginal or Torres Strait Islander Heritage	CALD	MUST MEET	MUST MEET at least one of the the following criteria					
											Applicant has or is eligible to hold an Australian Security Clearance (or recognised equivalent)	Legal Qualification and Experience	Professional experience in Cyber or Information Security	Significant experience in audit, assurance or review processes, public administration or financial or prudential regulation	Significant experience in incident management or crisis response	Significant experience in a critical infrastructure sector	Educational qualification in cyber security or information security
14	s. 22(1)(a)(ii)																
15																	
16																	
17																	
18																	
19																	
20																	

Cyber Incident Review Board																			
Applicant					Job Title		Location and Diversity				Eligibility Criteria								
											To be eligible for the Board, candidates must be able to obtain a NV1 level security clearance and meet at least one of the other eligibility criteria								
					MUST MEET at least one of the the following criteria														
					MUST MEET														
No.	Last Name	First Name	Title	Position Applied to	Position held	Company	State and Territory	Gender	Aboriginal or Torres Strait Islander Heritage	CALD	Applicant has or is eligible to hold an Australian Security Clearance (or recognised equivalent)	Legal Qualification and Experience	Professional experience in Cyber or Information Security	Significant experience in audit, assurance or review processes, public administration or financial or prudential regulation	Significant experience in incident management or crisis response	Significant experience in a critical infrastructure sector	Educational qualification in cyber security or information security	Academic qualifications or knowledge in a relevant field	Commonwealth, State or Territory government position at a senior level
21	s. 22(1)(a)(ii)																		
22																			
23																			
24																			
25																			
26																			
None																			

Cyber Incident Review Board																			
Applicant					Job Title		Location and Diversity			Eligibility Criteria									
										To be eligible for the Board, candidates must be able to obtain a NV1 level security clearance and meet at least one of the other eligibility criteria									
					MUST MEET at least one of the the following criteria														
No.	Last Name	First Name	Title	Position Applied to	Position held	Company	State and Territory	Gender	Aboriginal or Torres Strait Islander Heritage	CALD	Applicant has or is eligible to hold an Australian Security Clearance (or recognised equivalent)	Legal Qualification and Experience	Professional experience in Cyber or Information Security	Significant experience in audit, assurance, or review processes, public administration or financial or prudential regulation	Significant experience in Incident management or crisis response	Significant experience in a critical infrastructure sector	Educational qualification in cyber security or information security	Academic qualifications or knowledge in a relevant field	Commonwealth, State or Territory government position at a senior level
27	s. 22(1)(a)(ii)																		
28																			
29																			
30																			
31																			
32																			
33	22(1)(a)																		
34	22(1)(a)	s. 22(1)(a)(ii)																	

Cyber Incident Review Board																			
Applicant					Job Title		Location and Diversity				Eligibility Criteria								
											To be eligible for the Board, candidates must be able to obtain a NV1 level security clearance and meet at least one of the other eligibility criteria								
					MUST MEET at least one of the the following criteria														
					MUST MEET														
No.	Last Name	First Name	Title	Position Applied to	Position held	Company	State and Territory	Gender	Aboriginal or Torres Strait Islander Heritage	CALD	Applicant has or is eligible to hold an Australian Security Clearance (or recognised equivalent)	Legal Qualification and Experience	Professional experience in Cyber or Information Security	Significant experience in audit, assurance or review processes, public administration or financial or prudential regulation	Significant experience in incident management or crisis response	Significant experience in a critical infrastructure sector	Educational qualification in cyber security or information security	Academic qualifications or knowledge in a relevant field	Commonwealth, State or Territory government position at a senior level
35	s. 22(1)(a)(ii)																		
36																			
37																			
38																			
39																			
40																			
41																			
42	s. 22(1)(a)	s. 22(1)(a)(ii)																	
43	s. 22(1)																		

Cyber Incident Review Board																		
Applicant					Job Title		Location and Diversity				Eligibility Criteria							
											To be eligible for the Board, candidates must be able to obtain a NV1 level security clearance and meet at least one of the other eligibility criteria							
No.	Last Name	First Name	Title	Position Applied to	Position held	Company	State and Territory	Gender	Aboriginal or Torres Strait Islander Heritage	CALD	MUST MEET	MUST MEET at least one of the the following criteria						
											Applicant has or is eligible to hold an Australian Security Clearance (or recognised equivalent)	Legal Qualification and Experience	Professional experience in Cyber or Information Security	Significant experience in audit, assurance or review processes, public administration or financial or prudential regulation	Significant experience in incident management or crisis response	Significant experience in a critical infrastructure sector	Educational qualification in cyber security or information security	Academic qualifications or knowledge in a relevant field
44	s. 22(1)(a)(ii)																	
45																		
46																		
47																		
48																		
49																		
50																		

Cyber Incident Review Board																			
Applicant					Job Title		Location and Diversity			Eligibility Criteria									
										To be eligible for the Board, candidates must be able to obtain a NV1 level security clearance and meet at least one of the other eligibility criteria									
										MUST MEET at least one of the the following criteria									
No.	Last Name	First Name	Title	Position Applied to	Position held	Company	State and Territory	Gender	Aboriginal or Torres Strait Islander Heritage	CALD	MUST MEET	Legal Qualification and Experience	Professional experience in Cyber or Information Security	Significant experience in audit, assurance or review processes, public administration or financial or prudential regulation	Significant experience in incident management or crisis response	Significant experience in a critical infrastructure sector	Educational qualification in cyber security or information security	Academic qualifications or knowledge in a relevant field	Commonwealth, State or Territory government position at a senior level
51	s. 22(1)(a)(ii)																		
52																			
53																			
54																			
55																			
56																			
57																			

Cyber Incident Review Board																			
Applicant					Job Title		Location and Diversity				Eligibility Criteria								
											To be eligible for the Board, candidates must be able to obtain a NV1 level security clearance and meet at least one of the other eligibility criteria								
											MUST MEET	MUST MEET at least one of the the following criteria							
No.	Last Name	First Name	Title	Position Applied to	Position held	Company	State and Territory	Gender	Aboriginal or Torres Strait Islander Heritage	C&ID	Applicant has or is eligible to hold an Australian Security Clearance (or recognised equivalent)	Legal Qualification and Experience	Professional experience in Cyber or Information Security	Significant experience in audit, assurance or review processes, public administration or prudential regulation	Significant experience in incident management or crisis response	Significant experience in a critical infrastructure security sector	Educational qualification in cyber security or information security	Academic qualifications or knowledge in a relevant field	Commonwealth, State or Territory government position at a senior level
58	s. 22(1)(a)(ii)																		
59																			
60																			
61																			
62																			
63																			
64																			

Cyber Incident Review Board																			
Applicant					Job Title		Location and Diversity					Eligibility Criteria							
												To be eligible for the Board, candidates must be able to obtain a NV1 level security clearance and meet at least one of the other eligibility criteria							
					MUST MEET at least one of the the following criteria														
MUST MEET																			
No.	Last Name	First Name	Title	Position Applied to	Position held	Company	State and Territory	Gender	Aboriginal or Torres Strait Islander Heritage	CALD	Applicant has or is eligible to hold an Australian Security Clearance (or recognised equivalent)	Legal Qualification and Experience	Professional experience in Cyber or Information Security	Significant experience in audit, assurance or review processes, public administration or financial or prudential regulation	Significant experience in incident management or crisis response	Significant experience in a critical infrastructure sector	Educational qualification in cyber security or Information security	Academic qualifications or knowledge in a relevant field	Commonwealth, State or Territory government position at a senior level
65	s. 22(1)(a)(ii)																		
66																			
67																			
68																			
69																			
70																			
71																			

Cyber Incident Review Board																			
Applicant					Job Title		Location and Diversity				Eligibility Criteria								
											To be eligible for the Board, candidates must be able to obtain a NV1 level security clearance and meet at least one of the other eligibility criteria								
											MUST MEET at least one of the the following criteria								
MUST MEET																			
No.	Last Name	First Name	Title	Position Applied to	Position held	Company	State and Territory	Gender	Aboriginal or Torres Strait Islander Heritage	CALD	Applicant has or is eligible to hold an Australian Security Clearance (or recognised equivalent)	Legal Qualification and Experience	Professional experience in Cyber or Information Security	Significant experience in audit, assurance or review processes, public administration or financial or prudential regulation	Significant experience in incident management or crisis response	Significant experience in a critical infrastructure sector	Educational qualification in cyber security or information security	Academic qualifications or knowledge in a relevant field	Commonwealth, State or Territory government position at a senior level
72	s. 22(1)(a)(ii)																		
73																			
74																			
75																			
76																			
77																			
78																			

Cyber Incident Review Board																			
Applicant					Job Title		Location and Diversity				Eligibility Criteria								
											To be eligible for the Board, candidates must be able to obtain a NV1 level security clearance and meet at least one of the other eligibility criteria								
					MUST MEET at least one of the the following criteria														
MUST MEET																			
No.	Last Name	First Name	Title	Position Applied to	Position held	Company	State and Territory	Gender	Aboriginal or Torres Strait Islander Heritage	CALD	Applicant has or is eligible to hold an Australian Security Clearance (or recognised equivalent)	Legal Qualification and Experience	Professional experience in Cyber or Information Security	Significant experience in audit, assurance or review processes, public administration or financial or prudential regulation	Significant experience in incident management or crisis response	Significant experience in a critical infrastructure sector	Educational qualification in cyber security or information security	Academic qualifications or knowledge in a relevant field	Commonwealth, State or Territory government position at a senior level
79	s. 22(1)(a)(ii)																		
80																			
81																			
82																			
83																			
84																			
85																			

Cyber Incident Review Board																			
Applicant					Job Title		Location and Diversity					Eligibility Criteria							
												To be eligible for the Board, candidates must be able to obtain a NV1 level security clearance and meet at least one of the other eligibility criteria							
					MUST MEET at least one of the the following criteria														
					MUST MEET														
No.	Last Name	First Name	Title	Position Applied to	Position held	Company	State and Territory	Gender	Aboriginal or Torres Strait Islander Heritage	CALD	Applicant has or is eligible to hold an Australian Security Clearance (or recognised equivalent)	Legal Qualification and Experience	Professional experience in Cyber or Information Security	Significant experience in audit, assurance or review processes, public administration or financial or prudential regulation	Significant experience in incident management or crisis response	Significant experience in a critical infrastructure sector	Educational qualification in cyber security or information security	Academic qualifications or knowledge in a relevant field	Commonwealth, State or Territory government position at a senior level
86	s. 22(1)(a)(ii)																		
87																			
88																			
89																			
90																			
91																			
92																			

Cyber Incident Review Board																			
Applicant					Job Title		Location and Diversity			Eligibility Criteria									
										To be eligible for the Board, candidates must be able to obtain a NV1 level security clearance and meet at least one of the other eligibility criteria									
										MUST MEET	MUST MEET at least one of the the following criteria								
No.	Last Name	First Name	Title	Position Applied to	Position held	Company	State and Territory	Gender	Aboriginal or Torres Strait Islander Heritage	CALD	Applicant has or is eligible to hold an Australian Security Clearance (or recognised equivalent)	Legal Qualification and Experience	Professional experience in Cyber or Information Security	Significant experience in audit, assurance or review processes, public administration or financial or prudential regulation	Significant experience in incident management or crisis response	Significant experience in a critical infrastructure sector	Educational qualification in cyber security or information security	Academic qualifications or knowledge in a relevant field	Commonwealth, State or Territory government position at a senior level
93	s. 22(1)(a)(ii)																		
94																			
95																			
Continued																			
96	s. 22(1)(a)(ii)																		
97																			
98																			

Cyber Incident Review Board																			
Applicant					Job Title		Location and Diversity				Eligibility Criteria								
											To be eligible for the Board, candidates must be able to obtain a NV1 level security clearance and meet at least one of the other eligibility criteria								
											MUST MEET at least one of the the following criteria								
MUST MEET																			
No	Last Name	First Name	Title	Position Applied to	Position held	Company	State and Territory	Gender	Aboriginal or Torres Strait Islander Heritage	CALD	Applicant has or is eligible to hold an Australian Security Clearance (or recognised equivalent)	Legal Qualification and Experience	Professional experience in Cyber or Information Security	Significant experience in audit, assurance or review processes, public administration or financial or prudential regulation	Significant experience in incident management or crisis response	Significant experience in a critical infrastructure sector	Educational qualification in cyber security or information security	Academic qualifications or knowledge in a relevant field	Commonwealth, State or Territory government position at a senior level
99	s. 22(1)(a)(ii)																		
100																			
101																			
102																			
103																			
104																			
105																			

Cyber Incident Review Board																			
Applicant					Job Title		Location and Diversity				Eligibility Criteria								
											To be eligible for the Board, candidates must be able to obtain a NV1 level security clearance and meet at least one of the other eligibility criteria								
					MUST MEET at least one of the the following criteria														
					MUST MEET														
No.	Last Name	First Name	Title	Position Applied to	Position held	Company	State and Territory	Gender	Aboriginal or Torres Strait Islander Heritage	CALD	Applicant has or is eligible to hold an Australian Security Clearance (or recognised equivalent)	Legal Qualification and Experience	Professional experience in Cyber or Information Security	Significant experience in audit, assurance or review processes, public administration or financial or prudential regulation	Significant experience in incident management or crisis response	Significant experience in a critical infrastructure sector	Educational qualification in cyber security or information security	Academic qualifications or knowledge in a relevant field	Commonwealth, State or Territory government position at a senior level
106	s. 22(1)(a)(ii)																		
107																			
108																			
109																			
110																			
111																			
112																			

Cyber Incident Review Board																			
Applicant					Job Title		Location and Diversity				Eligibility Criteria								
											To be eligible for the Board, candidates must be able to obtain a NV1 level security clearance and meet at least one of the other eligibility criteria								
					MUST MEET at least one of the the following criteria														
No.	Last Name	First Name	Title	Position Applied to	Position held	Company	State and Territory	Gender	Aboriginal or Torres Strait Islander Heritage	CALD	Applicant has or is eligible to hold an Australian Security Clearance (or recognised equivalent)	Legal Qualification and Experience	Professional experience in Cyber or Information Security	Significant experience in audit, assurance or review processes, public administration or financial or prudential regulation	Significant experience in incident management or crisis response	Significant experience in a critical infrastructure sector	Educational qualification in cyber security or information security	Academic qualifications or knowledge in a relevant field	Commonwealth, State or Territory government position at a senior level
113	s. 22(1)(a)(ii)																		
114																			
115																			
116																			
117																			
118																			
119																			

Cyber Incident Review Board																			
Applicant				Job Title		Location and Diversity				Eligibility Criteria									
										To be eligible for the Board, candidates must be able to obtain a NV1 level security clearance and meet at least one of the other eligibility criteria:									
				MUST MEET at least one of the the following criteria															
No.	Last Name	First Name	Title	Position Applied to	Position held	Company	State and Territory	Gender	Aboriginal or Torres Strait Islander Heritage	CALD	MUST MEET	Legal Qualification and Experience	Professional experience in Cyber or Information Security	Significant experience in audit, assurance or review processes, public administration or financial or prudential regulation	Significant experience in incident management or crisis response	Significant experience in a critical infrastructure sector	Educational qualification in cyber security or information security	Academic qualifications or knowledge in a relevant field	Commonwealth, State or Territory government position at a senior level
120	s. 22(1)(a)(ii)																		
Security Australia																			
121	s. 22(1)(a)(ii)																		
122	s. 22(1)(a)(ii)																		
123	s. 22(1)(a)(ii)																		
124	s. 22(1)(a)(ii)																		
125	s. 22(1)(a)(ii)																		

Cyber Incident Review Board																			
Applicant					Job Title		Location and Diversity				Eligibility Criteria								
											To be eligible for the Board, candidates must be able to obtain a NV1 level security clearance and meet at least one of the other eligibility criteria								
					MUST MEET at least one of the the following criteria														
No.	Last Name	First Name	Title	Position Applied to	Position held	Company	State and Territory	Gender	Aboriginal or Torres Strait Islander Heritage	CALD	Applicant has or is eligible to hold an Australian Security Clearance (or recognised equivalent)	Legal Qualification and Experience	Professional experience in Cyber or Information Security	Significant experience in audit, assurance or review processes, public administration or financial or prudential regulation	Significant experience in incident management or crisis response	Significant experience in a critical infrastructure sector	Educational qualification in cyber security or information security	Academic qualifications or knowledge in a relevant field	Commonwealth, State or Territory government position at a senior level
126	s. 22(1)(a)(ii)																		
127																			
Victoria																			
128	s. 22(1)(a)(ii)																		
129																			
130	s. 22(1)(a)(ii)																		
131																			

Cyber Incident Review Board																		
Applicant					Job Title		Location and Diversity				Eligibility Criteria							
											To be eligible for the Board, candidates must be able to obtain a NV1 level security clearance and meet at least one of the other eligibility criteria							
No.	Last Name	First Name	Title	Position Applied to	Position held	Company	State and Territory	Gender	Aboriginal or Torres Strait Islander Heritage	CALD	MUST MEET	MUST MEET at least one of the the following criteria						
											Applicant has or is eligible to hold an Australian Security Clearance (or recognised equivalent)	Legal Qualification and Experience	Professional experience in Cyber or Information Security	Significant experience in audit, assurance or review processes, public administration or financial or prudential regulation	Significant experience in incident management or crisis response	Significant experience in a critical infrastructure sector	Educational qualification in cyber security or information security	Academic qualifications or knowledge in a relevant field
132	s. 22(1)(a)(ii)																	
133																		
134																		
135																		
136																		
137																		
138																		

Cyber Incident Review Board																			
Applicant					Job Title		Location and Diversity				Eligibility Criteria								
											To be eligible for this Board, candidates must be able to obtain a NV1 level security clearance and meet at least one of the other eligibility criteria								
											MUST MEET at least one of the the following criteria								
MUST MEET																			
No.	Last Name	First Name	Title	Position Applied to	Position held	Company	State and Territory	Gender	Aboriginal or Torres Strait Islander Heritage	CALD	Applicant has or is eligible to hold an Australian Security Clearance (or recognised equivalent)	Legal Qualification and Experience	Professional experience in Cyber or Information Security	Significant experience in audit, assurance or review processes, public administration or financial or prudential regulation	Significant experience in incident management or crisis response	Significant experience in a critical infrastructure sector	Educational qualification in cyber security or information security	Academic qualifications or knowledge in a relevant field	Commonwealth, State or Territory government position at a senior level
139	s. 22(1)(a)(ii)																		
140																			
141																			
142																			
143																			
144																			
145																			

Cyber Incident Review Board																			
Applicant					Job Title		Location and Diversity				Eligibility Criteria								
											To be eligible for the Board, candidates must be able to obtain a NV1 level security clearance and meet at least one of the other eligibility criteria								
										MUST MEET	MUST MEET at least one of the the following criteria								
No.	Last Name	First Name	Title	Position Applied to	Position Held	Company	State and Territory	Gender	Aboriginal or Torres Strait Islander Heritage	CALD	Applicant has or is eligible to hold an Australian Security Clearance (or recognised equivalent)	Legal Qualification and Experience	Professional experience in Cyber or Information Security	Significant experience in audit, assurance or review processes, public administration or financial or prudential regulation	Significant experience in incident management or crisis response	Significant experience in a critical infrastructure sector	Educational qualification in cyber security or information security	Academic qualifications or knowledge in a relevant field	Commonwealth, State or Territory government position at a senior level
146	s. 22(1)(a)(ii)																		
147																			
148																			
149																			
150																			
151		s. 22(1)(a)(ii)																	
152	s. 22(1)(a)(ii)																		

Cyber Incident Review Board																			
Applicant				Job Title		Location and Diversity			Eligibility Criteria To be eligible for the Board, candidates must be able to obtain a NV1 level security clearance and meet at least one of the other eligibility criteria										
No.	Last Name	First Name	Title	Position Applied to	Position held	Company	State and Territory	Gender	Aboriginal or Torres Strait Islander Heritage	CALD	MUST MEET	MUST MEET at least one of the the following criteria							
											Applicant has or is eligible to hold an Australian Security Clearance (or recognised equivalent)	Legal Qualification and Experience	Professional experience in Cyber or Information Security	Significant experience in audit, assurance or review processes, public administration or financial or prudential regulation	Significant experience in incident management or crisis response	Significant experience in a critical infrastructure sector	Educational qualification in cyber security or information security	Academic qualifications or knowledge in a relevant field	Commonwealth, State or Territory government position at a senior level
153	s. 22(1)(a)(ii)																		
154																			
155																			
156																			
157																			
158	s. 22(1)(a)(ii)																		
159																			

Cyber Incident Review Board																			
Applicant				Job Title		Location and Diversity					Eligibility Criteria								
											To be eligible for the Board, candidates must be able to obtain a NV1 level security clearance and meet at least one of the other eligibility criteria								
				MUST MEET at least one of the following criteria															
				MUST MEET															
No.	Last Name	First Name	Title	Position Applied to	Position held	Company	State and Territory	Gender	Aboriginal or Torres Strait Islander Heritage	CALD	Applicant has or is eligible to hold an Australian Security Clearance (or recognised equivalent)	Legal Qualification and Experience	Professional experience in Cyber or Information Security	Significant experience in audit, assurance or review processes, public administration or financial or prudential regulation	Significant experience in incident management or crisis response	Significant experience in a critical infrastructure sector	Educational qualification in cyber security or information security	Academic qualifications or knowledge in a relevant field	Commonwealth, State or Territory government position at a senior level
160	s. 22(1)																		
161																			
162																			
163																			
164																			
165																			
166																			

Cyber Incident Review Board																			
Applicant					Job Title		Location and Diversity				Eligibility Criteria								
											To be eligible for the Board, candidates must be able to obtain a NV1 level security clearance and meet at least one of the other eligibility criteria								
											MUST MEET	MUST MEET at least one of the the following criteria							
No.	Last Name	First Name	Title	Position Applied to	Position held	Company	State and Territory	Gender	Aboriginal or Torres Strait Islander Heritage	CALD	Applicant has or is eligible to hold an Australian Security Clearance (or recognised equivalent)	Legal Qualification and Experience	Professional experience in Cyber or Information Security	Significant experience in audit, assurance or review processes, public administration or financial or prudential regulation	Significant experience in incident management or crisis response	Significant experience in a critical infrastructure sector	Educational qualification in cyber security or information security	Academic qualifications or knowledge in a relevant field	Commonwealth, State or Territory government position at a senior level
167	s. 22(1)(a)(ii)																		
168																			
169																			
170																			
171																			
172																			
173																			

Cyber Incident Review Board																			
Applicant					Job Title		Location and Diversity				Eligibility Criteria								
											To be eligible for the Board, candidates must be able to obtain a NV1 level security clearance and meet at least one of the other eligibility criteria								
											MUST MEET	MUST MEET at least one of the the following criteria							
No.	Last Name	First Name	Title	Position Applied to	Position held	Company	State and Territory	Gender	Aboriginal or Torres Strait Islander Heritage	CALD	Applicant has or is eligible to hold an Australian Security Clearance (or recognised equivalent)	Legal Qualification and Experience	Professional experience in Cyber or Information Security	Significant experience in audit, assurance or review processes, public administration or financial or prudential regulation	Significant experience in incident management or crisis response	Significant experience in a critical infrastructure sector	Educational qualification in cyber security or information security	Academic qualifications or knowledge in a relevant field	Commonwealth, State or Territory government position at a senior level
174	s. 22(1)(a)(ii)																		
175																			
176																			
177																			
178																			
179																			

Cyber Incident Review Board																			
Applicant					Job Title		Location and Diversity				Eligibility Criteria								
											To be eligible for the Board, candidates must be able to obtain a NV1 level security clearance and meet at least one of the other eligibility criteria								
											MUST MEET	MUST MEET at least one of the the following criteria							
No.	Last Name	First Name	Title	Position Applied to	Position held	Company	State and Territory	Gender	Aboriginal or Torres Strait Islander Heritage	CALD	Applicant has or is eligible to hold an Australian Security Clearance (or recognised equivalent)	Legal Qualification and Experience	Professional experience in Cyber or Information Security	Significant experience in audit, assurance or review processes, public administration or financial or prudential regulation	Significant experience in incident management or crisis response	Significant experience in a critical infrastructure security sector	Educational qualification in cyber security or information security	Academic qualifications or knowledge in a relevant field	Commonwealth, State or Territory government position at a senior level
180	s. 22(1)(a)(ii)																		
181																			
182																			
183																			
184																			
185																			



OFFICIAL

Cyber Incident Review Board Membership and Skills Matrix Framework

Purpose

This Framework will be used to ensure that appointments to the Cyber Incident Review Board (the Board) and Expert Panel meet the eligibility criteria established in the *Cyber Security (Cyber Incident Review Board) Rules 2025* (the Rules) and support a fair and independent process for appointments to the Board.

The Framework will also ensure that the Board reflects the diversity of the Australian community and business sector, both in professional experience, as well as in gender, cultural background and age.

Background

The *Cyber Security Act 2024* (the Act) provides that the Minister is responsible for appointing the standing members of the Board, including the Chair. Once appointed, the Chair will make appointments to the Expert Panel. Eligibility criteria for both groups are set out in the Rules. **(Annex A)**

High profile cyber incidents, such as the Optus and MediBank breaches show the need for stronger action by government and industry to improve Australia's cyber resilience. The Board will review similar incidents and deliver reports and recommendations to government and industry which will uplift cyber resilience.

The Matrix helps the Chair ensure the right mix of skills and experience across the Board and Expert Panel to deliver these reports.

Role of the Secretariat

The Secretariat is responsible for management of the Matrix, including the receipt, triage and storage of information provided by current and prospective members of the Board and Expert Panel.

Receiving Information

Information provided by prospective or current members of the Board and Expert Panel for the purposes of demonstrating eligibility for appointment must be provided in writing to CIRB.Enquiries@homeaffairs.gov.au using the approved template. The Secretariat will pre-assess each individual's skills and capabilities before providing the pre-assessment and template to the Board for review and certification using the Matrix. The Board may assess the information at a meeting of the Board or out of session. Once the Board makes a final determination, the Secretariat will update the Cyber Incident Review Board Skills Register (the Register) as required.

Released by Department of Home Affairs
under the Freedom of Information Act 1982

OFFICIAL

Right to Review

A member of the Board or Expert Panel may request that their assessed skills or competencies be reviewed at any time by making a written request to CIRB.Enquiries@homeaffairs.gov.au and providing evidence of a new qualification or any other relevant factor. In these instances, the Secretariat will pre-assess the updated information and provide the updated information to the Board at its next meeting.

Information Storage and Access Controls

The Secretariat is responsible for managing the secure storage and access of the information submitted to the Board and stored within the Register. All information, and the Register itself, will be maintained on the Department's approved information management system (Content Manager). Access to Content Manager will be limited to the Chair and Secretariat.

Requirement to hold a security clearance

A person may be appointed as a standing member of the Board or Expert Panel, if, in addition to meeting the eligibility criteria set out in sections 13 and 22 of the Rules (**Annex A**), the person either:

- holds, or is eligible to hold, an Australian Government security clearance that allows the person access to information that has a security classification of at least secret level (NV1); or
- holds an equivalent security clearance recognised by the Commonwealth for the purposes of allowing the person access to information that has an NV1 security classification.

In order to be eligible for an Australian Government security clearance, an individual must:

- be an Australian citizen; and
- have a checkable background.

Appointment to the Board and Expert Panel

A person's eligibility for appointment to the Board and Expert Panel is established in the Rules. No individual member of the Board or Expert Panel is expected to have all the identified skills and experience; instead they must demonstrate 'significant' experience or qualifications in one or more of the listed skills.

The Matrix Assessment Tool (**Annex B**) establishes clear definitions of 'significant experience' for the purposes of determining if a potential appointee meets minimum thresholds for appointment, and also to grade any other relevant skills.

To meet the criteria for appointment person is required to score a '4' against one or more of the eligibility criteria.

Appointment to a Review Panel

Once the Board decides to conduct a review of a cyber incident, it forms a Review Panel. The Board will first review the skills and experience of the members of the Board and identify what additional skills and perspectives it requires to conduct the review. It will then seek to address those gaps by appointing members of the Expert Panel to the Review Panel.

Annual Review

The cyber threat landscape continues to evolve as businesses integrate new technologies into their networks and supply chains. To ensure that the Board continues to have the correct mix of skills, expertise and experience to fulfil its function in a dynamic environment. The Board will review both the skills matrix

assessment tool and the skills register to ensure that it remains fit for purpose and identify skills gaps to be addressed through new appointments.

Released by Department of Home Affairs
under the *Freedom of Information Act 1982*

Annex A – Cyber Security (Cyber Incident Review Board) Rules eligibility criteria

Section 13 Eligibility for appointment as a Board member

- (1) A person is only eligible to be appointed as a Board member, under section 64 or 66 of the Act, if:
- (a) the person either:
 - (i) holds, or is eligible to hold, an Australian Government security clearance that allows the person access to information that has a security classification of at least secret; or
 - (ii) holds an equivalent security clearance recognised by the Commonwealth for the purposes of allowing the person access to information that has a security classification of at least secret; and
 - (b) the person:
 - (i) has obtained a degree from a university, or an educational qualification of a similar standing, in the field of law and has significant experience working in that field; or
 - (ii) has obtained an educational qualification in the field of cyber security or information security; or
 - (iii) has significant experience working in the field of cyber security or information security; or
 - (iv) holds a relevant Commonwealth, State or Territory government position at an appropriately senior level; or
 - (v) has significant experience in audit, assurance or review processes, public administration or financial or prudential regulation; or
 - (vi) has significant experience in incident management or crisis response; or
 - (vii) has significant experience in a critical infrastructure sector (within the meaning of the Security of Critical Infrastructure Act 2018); or
 - (viii) has significant academic qualifications or knowledge in a relevant field.
- (2) Before appointing a person as a Board member, the Minister must be satisfied that:
- (a) the person meets the eligibility requirements mentioned in subsection (1); and
 - (b) the person has appropriate qualifications, knowledge, skills or experience to perform the role.
- (3) The Minister may appoint a person who holds a State or Territory government position only with the agreement of the State or Territory concerned.

Section 22 Appointments to the Expert Panel

- (3) A person is only eligible to be appointed as a member of the Expert Panel if:
- (a) the person either:
 - (i) holds, or is eligible to hold, an Australian Government security clearance that allows the person access to information that has a security classification of at least secret; or
 - (ii) holds an equivalent security clearance recognised by the Commonwealth for the purposes of allowing the person access to information that has a security classification of at least secret; and
 - (b) the person:
 - (i) has obtained a degree from a university, or an educational qualification of a similar standing, in the field of law and has significant experience working in that field; or
 - (ii) has obtained an educational qualification in the field of cyber security, information technology, computer networks or software engineering; or
 - (iii) has significant experience working in the field of cyber security or information security; or
 - (iv) holds a relevant Commonwealth, State or Territory government position at an appropriately senior level; or
 - (v) has significant experience in audit, assurance or review processes, public administration or financial or prudential regulation; or

 Released by Department of Home Affairs
under the Freedom of Information Act 1982

- (vi) has significant experience in incident management or crisis response;
 - (vii) has significant experience in a critical infrastructure sector (within the meaning of the Security of Critical Infrastructure Act 2018); or
 - (viii) has significant academic qualifications or knowledge in a relevant field.
- (4) Before appointing a person as a member of the Expert Panel, the Chair must be satisfied that:
- (a) the person meets the eligibility requirements mentioned in subsection (3); and
 - (b) the person has appropriate qualifications, knowledge, skills or experience to perform the role.
- (5) The Chair may appoint a person who holds a State or Territory government position only with the agreement of the State or Territory concerned.

Annex B – Skills Matrix Assessment Tool

<u>Competence Score</u>	<u>Description</u>
<u>1 – Limited</u>	The individual has no formal work experience, knowledge or qualifications in the skill.
<u>2 - Background</u>	The individual has had some ancillary/indirect exposure through work experience or training sufficient to enable background awareness but not sound knowledge. For example, exposure to the skill's subject matter while working in a different function that the skill is connected to.
<u>3 - Sound</u>	The individual has had experience or training sufficient to give a sound understanding of the skill. This includes (but is not limited to) having had: • relevant work experience of at least 2 years, specific to the skill; or • relevant training in relation to the skill below a tertiary level, such as through short courses, industry conferences, seminars or in-house training programs
<u>4 - Comprehensive</u>	The individual has significant experience or holds relevant qualifications that give a comprehensive understanding of the skill. This includes (but is not limited to) having: • had relevant work experience of at least 5 years specific to the skill in an area either specifically relevant or transferrable to the work, including experience on boards at a management level or in a professional services firm; or • holds tertiary qualifications or industry equivalents specific to the skill.
<u>5 - Professional/Expert</u>	The individual has had significant experience and generally also holds relevant qualifications to give an expert understanding of the skill. This includes (but is not limited to) having had: • relevant work experience of at least 10 years specific to the skill, including experience on boards, at a senior management level, or in a professional services firm; and • holds tertiary qualifications or industry equivalents specific to the skill. Where a person has significant experience (of over 15 years) a qualification is not necessary if that particular skill does not require a professional qualification. For example, while a lawyer would be required to have a law degree and years of experience practising law to score a 5 for the legal skill. A senior security or project manager may not be required to hold a qualification in order to be graded at this level.

OFFICIAL: Sensitive

Australian Government
Department of Home Affairs

Submission

For decision

PDMS Ref. Number: MS25-004340

Date of Clearance: 23/04/2026

To Minister for Home Affairs, Minister for Immigration and Citizenship,
 Minister for Cyber Security

Subject Cyber Incident Review Board Appointments

Timing *No later than 28 April 2026, for the proposed appointments of the Chair and other members of the Cyber Incident Review Board to commence on 1 May 2026. A waiver to the 10 day clearance rule was provided by your office.*

Recommendations

That you:

1. sign the instrument of appointment for the Chair of the Cyber Incident Review Board (the Board) in order for the proposed appointment to commence on 1 May 2026 (**Attachment A1**); signed / not signed
2. sign the instruments of appointment for the 6 standing members of the Board in order for the proposed appointments to commence on 1 May 2026 (**Attachment A2** to **Attachment A7**); signed / not signed
3. sign the appointment letters for the Board members (**Attachment B1** to **Attachment B7**); and signed / not signed
4. note that the timing for announcement of the appointments will be settled with your office. noted / please discuss

Minister for Home Affairs, Minister for Immigration and
 Citizenship, Minister for Cyber Security

Signature.....

Date:...../...../2026

284

OFFICIAL: Sensitive

Minister's Comments

Key Issues

1. This submission seeks your agreement to formally appoint the approved candidates as Chair and standing members of the Cyber Incident Review Board (the Board) by signing the instruments of appointment (Attachment A1 to Attachment A7).
2. Under the *Cyber Security Act 2024* (the Act), you must appoint the Chair and standing members of the Board by written instrument.
 - Section 61 of the Act provides that the Board consists of a Chair and at least 2 but no more than 6 other standing members.
3. On 16 April 2026, the Assistant Minister to the Prime Minister, the Hon Patrick Gorman MP, approved the proposed appointment of your preferred candidates to the Board (**MS25-003313** refers).
4. Consistent with the approval from the Assistant Minister to the Prime Minister, the intention is for all 7 approved appointments to commence on 1 May 2026, for a period of 4 years (the maximum period available under the Act). All 7 appointments would be on a part-time basis.
5. The approved candidates are:

Approved candidate for Chair

- s. 22(1)(a)(ii)

Approved candidates for standing members

s. 22(1)(a)(ii)

6. This submission also seeks your agreement to issue appointment letters to the approved candidates, with the signed instruments of appointment attached (**Attachment B1 to Attachment B7**). The letters will also include Incoming Chair and Standing Member Briefs which will provide Board members with information about the role, secretariat, governance and remuneration (**Attachment C** and **Attachment D**).

Next steps to finalise appointments

7. Should you agree to sign the instruments of appointment and the once letters have been sent, the Department of Home Affairs' (the Department) Communications and Media team will settle timing of the media release announcing the appointments with your office.
8. The Department will also lodge the signed instruments of appointment for registration on the Federal Register of Legislation as notifiable instruments, which will be publicly accessible. Registration will occur within 2 business days of signing unless your office advises otherwise.
9. The Department will work with your office to schedule an introductory meeting between you and the Chair to ensure early alignment on priorities, expectations and the Board's commencement approach.

Standing up the new Board and settling governance matters

10. Once appointed, the Board may begin considering referrals for review. Before commencing its first review, the Board must finalise internal governance arrangements and agree to a review methodology.
 - The Department has prepared a suite of draft governance materials to support the Board's consideration of these matters.
11. The Board will also need to establish an Expert Panel to support review activities, with members of the Expert Panel to be appointed by the Chair.
 - The Expert Panel will comprise industry leaders, technical specialists, academics and practitioners, appointed through a transparent, merit-based process.
 - The Department will support the Board to establish the Expert Panel leveraging the existing Expression of Interest process and register from the Board appointment process.
 - The Board may commence its first review while Expert Panel appointments are being finalised.
12. Once established, the Board will then prepare a draft Terms of Reference (ToR) for any proposed review for your consideration and approval.
 - The ToR will outline the review's scope, objectives, timeframes, key lines of inquiry and any specialist expertise the Board intends to draw upon.
 - The Department will work with the Board to ensure the ToR are robust, consistent with legislative requirements and aligned with your expectations.

Background

13. All proposed appointees hold or are eligible to hold a security clearance and have the appropriate knowledge, skills or experience for their roles, and therefore meet the prescribed eligibility requirements outlined in the Rules.
 - On 18 March 2026, the Department provided you with each candidate's curriculum vitae which illustrates their suitability under paragraph 13(1)(b), as well as their private interest declarations and due diligence background checks (**MS26-000559** refers).
 - No conflicts of interest or adverse findings were identified that would compromise any candidate's ability to perform their duties as a Board member.

Consultation–Internal/External

14. **Internal:** Legal Group have been consulted on the preparation of the written instruments of appointment and this submission.

Risks and Sensitivities

15. The Board is established under Part 5 of the Act, with eligibility, appointment and operational requirements prescribed by Rules. The legislation commenced on 29 May 2025. Interest in the timing of the Board's establishment is increasing, reflecting stakeholder expectations regarding the commencement of the Board's statutory functions. The Department is managing these expectations through regular website updates and ongoing stakeholder consultation.
16. The expression of interest exercise was conducted under an exemption from the Government's Merit and Transparency Policy, granted by the Prime Minister, which may give rise to concerns that the appointments were not merit-based. The Department has implemented measures to replicate the Policy's usual processes, including an independent, transparent and merit-based assessment of candidates.

Media implications

17. The Department's Media and Communications Branch will settle details and timing of the media release with your office.

Legal Implications

18. The written instruments of appointment must be signed before the terms of the Chair and standing members are proposed to commence on 1 May 2026.

Attachments

Attachments A Written Instrument of Appointment

• s. 22(1)(a)(ii)
•
•
•
•
•
•

Attachments B Candidate Letter of offer, accompanied by written Instruments of Appointment and information pack

• s. 22(1)(a)(ii)
•
•
•
•
•
•

Attachment C Incoming Chair Brief to be attached to letter B1 - s. 22(1)(a)(ii)

Attachment D Appointment Information Pack to be attached to letters:

• s. 22(1)(a)(ii)
•
•
•
•
•
•

Authorising Officer
Cleared by
Greta Doherty Acting Deputy Secretary Law Enforcement & Domestic Security Group
Date: 23/04/2026 Mob. s. 22(1)(a)(ii)

Contact Officer Ms Georgina Papoutsis, Acting Assistant Secretary, Cyber Policy & Programs Branch, Mob, s. 22(1)(a)(ii)

CC Head of National Security
 DS Chief Operating Officer
 DS Executive
 DS Legal
 FAS CFICT
 FAS Executive Coordination
 AS Legislation

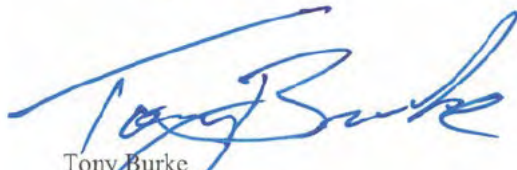


ADMIN 26/102

Cyber Security (Chair of the Cyber Incident Review Board) Appointment 2026

I, Tony Burke, Minister for Home Affairs and Minister for Cyber Security, under section 64 of the *Cyber Security Act 2024*, appoint **s. 22(1)(a)(ii)** as the Chair of the Cyber Incident Review Board, on a part-time basis, for the period of 4 years that begins on 1 May 2026.

Dated 28.4 2026



Tony Burke
Minister for Home Affairs
Minister for Cyber Security



ADMIN 26/103

Cyber Security (Member of the Cyber Incident Review Board) Appointment (No. 1) 2026

I, Tony Burke, Minister for Home Affairs and Minister for Cyber Security, under section 66 of the *Cyber Security Act 2024*, appoint **22(1)(a)(ii)** as a standing member of the Cyber Incident Review Board, on a part-time basis, for the period of 4 years that begins on 1 May 2026.

Dated **28.4** 2026

A blue ink signature of Tony Burke, written in a cursive style.

Tony Burke
Minister for Home Affairs
Minister for Cyber Security

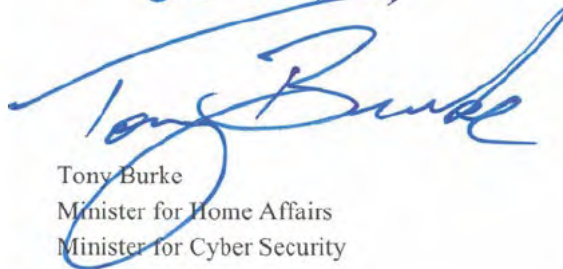


ADMIN 26/104

Cyber Security (Member of the Cyber Incident Review Board) Appointment (No. 2) 2026

I, Tony Burke, Minister for Home Affairs and Minister for Cyber Security, under section 66 of the *Cyber Security Act 2024*, appoint **s. 22(1)(a)(ii)** as a standing member of the Cyber Incident Review Board, on a part-time basis, for the period of 4 years that begins on 1 May 2026.

Dated 28.4 2026



Tony Burke
Minister for Home Affairs
Minister for Cyber Security



ADMIN 26/105

Cyber Security (Member of the Cyber Incident Review Board) Appointment (No. 3) 2026

I, Tony Burke, Minister for Home Affairs and Minister for Cyber Security, under section 66 of the *Cyber Security Act 2024*, appoint **s. 22(1)(a)(ii)** as a standing member of the Cyber Incident Review Board, on a part-time basis, for the period of 4 years that begins on 1 May 2026.

Dated 28.4 2026

A handwritten signature in blue ink, reading "Tony Burke".

Tony Burke
Minister for Home Affairs
Minister for Cyber Security



ADMIN 26/106

Cyber Security (Member of the Cyber Incident Review Board) Appointment (No. 4) 2026

I, Tony Burke, Minister for Home Affairs and Minister for Cyber Security, under section 66 of the *Cyber Security Act 2024*, appoint **s. 22(1)(a)(ii)** as a standing member of the Cyber Incident Review Board, on a part-time basis, for the period of 4 years that begins on 1 May 2026.

Dated 28.9 2026


Tony Burke
Minister for Home Affairs
Minister for Cyber Security



ADMIN 26/107

Cyber Security (Member of the Cyber Incident Review Board) Appointment (No. 5) 2026

I, Tony Burke, Minister for Home Affairs and Minister for Cyber Security, under section 66 of the *Cyber Security Act 2024*, appoint **22(1)(a)(ii)** as a standing member of the Cyber Incident Review Board, on a part-time basis, for the period of 4 years that begins on 1 May 2026.

Dated **28.4** 2026

Tony Burke
Minister for Home Affairs
Minister for Cyber Security

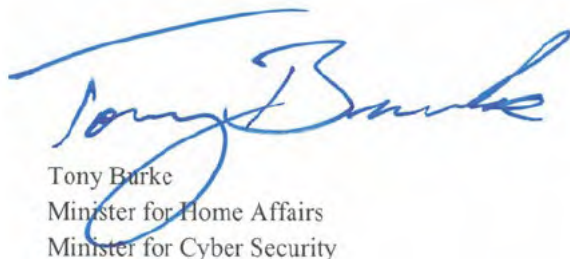


ADMIN 26/108

Cyber Security (Member of the Cyber Incident Review Board) Appointment (No. 6) 2026

I, Tony Burke, Minister for Home Affairs and Minister for Cyber Security, under section 66 of the *Cyber Security Act 2024*, appoint **22(1)(a)(ii)** as a standing member of the Cyber Incident Review Board, on a part-time basis, for the period of 4 years that begins on 1 May 2026.

Dated **28.4** 2026



Tony Burke
Minister for Home Affairs
Minister for Cyber Security



The Hon Tony Burke MP
Minister for Home Affairs
Minister for Immigration and Citizenship
Minister for Cyber Security
Minister for the Arts
Leader of the House

Ref No: MS25-004340

s. 22(1)(a)(ii)

Dear s. 22(1)(a)(ii)

Thank you for your recent expression of interest in serving on the Cyber Incident Review Board (the Board). I am pleased to congratulate you on your appointment as Chair.

Please find attached the signed written instrument of appointment, along with the Incoming Chair Brief, which outlines key details for your commencement, including Board membership, your remuneration arrangements, the anticipated meeting schedule and key secretariat contacts.

As Chair, you will lead an expert independent body that reviews significant cyber incidents, identifies lessons learned, and develops recommendations to enhance Australia's economic prosperity, national security and social cohesion.

The Board will be established from May 2026 and will comprise some of Australia's most experienced leaders and experts in cyber security. It will play a pivotal role in bringing government, industry and the community together to strengthen national cyber security and resilience.

The Department of Home Affairs will support the Board through a dedicated secretariat. The secretariat will assist with the establishment and operations of the Board. It will also work with you to schedule an introductory meeting with me – to ensure early alignment on priorities, expectations and the Board's commencement approach.

If you have any questions regarding the appointment process, your role, remuneration or the Board's operations, please contact the secretariat directly by email at CIRB.Enquiries@homeaffairs.gov.au.

Congratulations once again on your appointment as Chair and thank you for your commitment to enhancing Australia's cyber security resilience.

Yours sincerely



Tony Burke

28 / 4 / 2026

Encl: Written Instrument of Appointment
Cyber Incident Review Board – Incoming Chair Brief



The Hon Tony Burke MP
Minister for Home Affairs
Minister for Immigration and Citizenship
Minister for Cyber Security
Minister for the Arts
Leader of the House

Ref No: MS25-004340

s. 22(1)(a)(ii)

Dear s. 22(1)(a)(ii)

Thank you for your recent expression of interest in serving on the Cyber Incident Review Board (the Board). I am pleased to congratulate you on your appointment as a standing member.

Please find attached the signed written instrument of appointment, along with the Appointment Information Pack, which outlines key details for your commencement, including Board membership, your remuneration arrangements, the anticipated meeting schedule and key secretariat contacts.

As a standing member, you will contribute to an expert independent body that reviews significant cyber security incidents, identifies lessons learned, and develops recommendations to enhance Australia's economic prosperity, national security and social cohesion.

The Board will be established from May 2026 and will comprise some of Australia's most experienced leaders and experts in cyber security. It will play a pivotal role in bringing government, industry and the community together to strengthen national cyber security and resilience.

The Department of Home Affairs will support the Board through a dedicated secretariat. The secretariat will contact you shortly with further information on the Board's commencement and operational arrangements.

If you have any questions regarding the appointment process, role, remuneration or the Board's operations, please contact the secretariat directly by email at CIRB.Enquiries@homeaffairs.gov.au.

Congratulations again on your appointment as a standing member and thank you for your commitment to strengthening cyber security resilience across the Australian economy.

Yours sincerely



Tony Burke

28 / 4 / 2026

Encl: Written Instrument of Appointment
Cyber Incident Review Board - Appointment Information Pack



The Hon Tony Burke MP
Minister for Home Affairs
Minister for Immigration and Citizenship
Minister for Cyber Security
Minister for the Arts
Leader of the House

Ref No: MS25-004340

s. 22(1)(a)(ii)

Dear s. 22(1)(a)(ii)

Thank you for your recent expression of interest in serving on the Cyber Incident Review Board (the Board). I am pleased to congratulate you on your appointment as a standing member.

Please find attached the signed written instrument of appointment, along with the Appointment Information Pack, which outlines key details for your commencement, including Board membership, your remuneration arrangements, the anticipated meeting schedule and key secretariat contacts.

As a standing member, you will contribute to an expert independent body that reviews significant cyber security incidents, identifies lessons learned, and develops recommendations to enhance Australia's economic prosperity, national security and social cohesion.

The Board will be established from May 2026 and will comprise some of Australia's most experienced leaders and experts in cyber security. It will play a pivotal role in bringing government, industry and the community together to strengthen national cyber security and resilience.

The Department of Home Affairs will support the Board through a dedicated secretariat. The Department will also sponsor and support you to obtain an Australian Government security clearance at the Negative Vetting 1 (NV1) level, which is required for participation in the Board's governance and review activities.

The secretariat will contact you shortly with further information on these arrangements and on the Board's commencement.

If you have any questions regarding the appointment process, role, remuneration or the Board's operations, please contact the secretariat directly by email at CIRB.Enquiries@homeaffairs.gov.au.

Congratulations again on your appointment as a standing member and thank you for your commitment to strengthening cyber security resilience across the Australian economy.

Yours sincerely



Tony Burke

28/4 / 2026

Encl: Written Instrument of Appointment
Cyber Incident Review Board - Appointment Information Pack



The Hon Tony Burke MP
Minister for Home Affairs
Minister for Immigration and Citizenship
Minister for Cyber Security
Minister for the Arts
Leader of the House

Ref No: MS25-004340

s. 22(1)(a)(ii)

Dear s. 22(1)(a)(ii)

Thank you for your recent expression of interest in serving on the Cyber Incident Review Board (the Board). I am pleased to congratulate you on your appointment as a standing member.

Please find attached the signed written instrument of appointment, along with the Appointment Information Pack, which outlines key details for your commencement, including Board membership, your remuneration arrangements, the anticipated meeting schedule and key secretariat contacts.

As a standing member, you will contribute to an expert independent body that reviews significant cyber security incidents, identifies lessons learned, and develops recommendations to enhance Australia's economic prosperity, national security and social cohesion.

The Board will be established from May 2026 and will comprise some of Australia's most experienced leaders and experts in cyber security. It will play a pivotal role in bringing government, industry and the community together to strengthen national cyber security and resilience.

The Department of Home Affairs will support the Board through a dedicated secretariat. The secretariat will contact you shortly with further information on the Board's commencement and operational arrangements.

If you have any questions regarding the appointment process, role, remuneration or the Board's operations, please contact the secretariat directly by email at CIRB.Enquiries@homeaffairs.gov.au.

Congratulations again on your appointment as a standing member and thank you for your commitment to strengthening cyber security resilience across the Australian economy.

Yours sincerely



Tony Burke

28/4/2026

Encl: Written Instrument of Appointment
Cyber Incident Review Board - Appointment Information Pack



The Hon Tony Burke MP
Minister for Home Affairs
Minister for Immigration and Citizenship
Minister for Cyber Security
Minister for the Arts
Leader of the House

Ref No: MS25-004340

s. 22(1)(a)(ii)

Dear **s. 22(1)(a)(ii)**

Thank you for your recent expression of interest in serving on the Cyber Incident Review Board (the Board). I am pleased to congratulate you on your appointment as a standing member.

Please find attached the signed written instrument of appointment, along with the Appointment Information Pack, which outlines key details for your commencement, including Board membership, your remuneration arrangements, the anticipated meeting schedule and key secretariat contacts.

As a standing member, you will contribute to an expert independent body that reviews significant cyber security incidents, identifies lessons learned, and develops recommendations to enhance Australia's economic prosperity, national security and social cohesion.

The Board will be established from May 2026 and will comprise some of Australia's most experienced leaders and experts in cyber security. It will play a pivotal role in bringing government, industry and the community together to strengthen national cyber security and resilience.

The Department of Home Affairs will support the Board through a dedicated secretariat. The secretariat will contact you shortly with further information on the Board's commencement and operational arrangements.

If you have any questions regarding the appointment process, role, remuneration or the Board's operations, please contact the secretariat directly by email at CIRB.Enquiries@homeaffairs.gov.au.

Congratulations again on your appointment as a standing member and thank you for your commitment to strengthening cyber security resilience across the Australian economy.

Yours sincerely



Tony Burke

28 / 4 / 2026

Encl: Written Instrument of Appointment
Cyber Incident Review Board - Appointment Information Pack



The Hon Tony Burke MP
Minister for Home Affairs
Minister for Immigration and Citizenship
Minister for Cyber Security
Minister for the Arts
Leader of the House

Ref No: MS25-004340

s. 22(1)(a)(ii)

Dear s. 22(1)(a)(ii)

Thank you for your recent expression of interest in serving on the Cyber Incident Review Board (the Board). I am pleased to congratulate you on your appointment as a standing member.

Please find attached the signed written instrument of appointment, along with the Appointment Information Pack, which outlines key details for your commencement, including Board membership, your remuneration arrangements, the anticipated meeting schedule and key secretariat contacts.

As a standing member, you will contribute to an expert independent body that reviews significant cyber security incidents, identifies lessons learned, and develops recommendations to enhance Australia's economic prosperity, national security and social cohesion.

The Board will be established from May 2026 and will comprise some of Australia's most experienced leaders and experts in cyber security. It will play a pivotal role in bringing government, industry and the community together to strengthen national cyber security and resilience.

The Department of Home Affairs will support the Board through a dedicated secretariat. The secretariat will contact you shortly with further information on the Board's commencement and operational arrangements.

If you have any questions regarding the appointment process, role, remuneration or the Board's operations, please contact the secretariat directly by email at CIRB.Enquiries@homeaffairs.gov.au.

Congratulations again on your appointment as a standing member and thank you for your commitment to strengthening cyber security resilience across the Australian economy.

Yours sincerely



Tony Burke

284 / 2026

Encl: Written Instrument of Appointment
Cyber Incident Review Board - Appointment Information Pack



The Hon Tony Burke MP
Minister for Home Affairs
Minister for Immigration and Citizenship
Minister for Cyber Security
Minister for the Arts
Leader of the House

Ref No: MS25-004340

s. 22(1)(a)(ii)

Dear **s. 22(1)(a)(ii)**

Thank you for your recent expression of interest in serving on the Cyber Incident Review Board (the Board). I am pleased to congratulate you on your appointment as a standing member.

Please find attached the signed written instrument of appointment, along with the Appointment Information Pack, which outlines key details for your commencement, including Board membership, your remuneration arrangements, the anticipated meeting schedule and key secretariat contacts.

As a standing member, you will contribute to an expert independent body that reviews significant cyber security incidents, identifies lessons learned, and develops recommendations to enhance Australia's economic prosperity, national security and social cohesion.

The Board will be established from May 2026 and will comprise some of Australia's most experienced leaders and experts in cyber security. It will play a pivotal role in bringing government, industry and the community together to strengthen national cyber security and resilience.

The Department of Home Affairs will support the Board through a dedicated secretariat. The secretariat will contact you shortly with further information on the Board's commencement and operational arrangements.

If you have any questions regarding the appointment process, role, remuneration or the Board's operations, please contact the secretariat directly by email at CIRB.Enquiries@homeaffairs.gov.au.

Congratulations again on your appointment as a standing member and thank you for your commitment to strengthening cyber security resilience across the Australian economy.

Yours sincerely



Tony Burke

28/4/2026

Encl: Written Instrument of Appointment
Cyber Incident Review Board - Appointment Information Pack



Australian Government
Cyber Incident Review Board

The Cyber Incident Review Board Incoming Chair Brief

1. Welcome to the Chair

I am pleased to welcome you to your role as Chair of the Cyber Incident Review Board. Your appointment represents an important step in strengthening Australia's ability to learn from major cyber security incidents and to build a more resilient national cyber environment.

The Government has established the Board to provide independent, expert insight into significant cyber incidents, and to support a culture of continuous improvement across sectors. Your leadership will be central to shaping how the Board approaches its work, engages with stakeholders, and contributes to a stronger and more informed national response to cyber threats.

As Chair, you will guide the Board's deliberations and ensure its reviews are conducted with the rigour, independence and professionalism expected of a statutory advisory body. The Government values the depth of experience you bring to this role and the perspective you will provide as the Board begins its important work.

You will be supported by a dedicated Secretariat, who will assist you in establishing the Board's operating arrangements and ensuring you have the information and resources required to carry out your functions effectively. The Department looks forward to working closely with you as you commence in the role.

Thank you for your willingness to serve in this capacity. I am confident that under your leadership, the Board will make a significant contribution to Australia's cyber security landscape.

Yours sincerely

Ashley Bell
Acting First Assistant Secretary,
Counter Foreign Interference, Cyber and Technology Division

2. Executive Summary

Australia's cyber security environment is evolving rapidly. As organisations deepen their digital reliance, expectations for strong cyber governance continue to rise, and many businesses are seeking clearer guidance on what effective cyber security looks like in practice. Recent major incidents have highlighted the need for a more consistent national approach to identifying vulnerabilities and embedding lessons learned across industry.

The Cyber Incident Review Board has been established under the *Cyber Security Act 2024* to address this need. As an independent, no-fault advisory body, the Board will examine significant cyber incidents and translate insights into practical, system wide recommendations that uplift national cyber resilience. Its work will complement existing regulatory, law enforcement and intelligence functions, providing a trusted mechanism to strengthen corporate governance, preparedness and response.

For you as the incoming Chair, this represents an opportunity to shape a new national capability that supports both government and industry. The Board's insights will feed into Australia's broader threat intelligence, awareness and exercise programs, making early leadership critical to ensuring its guidance is targeted, credible and impactful. Strong early stewardship will lay the foundations for a Board that materially improves national cyber resilience.

This Incoming Chair Brief Pack outlines the Board's purpose, structure and operating arrangements, and provides key information to support your commencement.

As an initial priority, in setting up the Board, there are several foundational decisions and actions that will be required to establish the Board's operating rhythm, governance settings and stakeholder relationships.

These include convening the inaugural Board meeting, engaging key Departmental and Government stakeholders and establishing the process for forming the Expert Panel pool.

Board members will have well defined expectations and a shared understanding of priorities, anchored by a clear strategic outlook for the first 12 months. As Chair, you will also have established a productive and collaborative partnership with the Board secretariat to ensure effective operations and informed oversight.

Once established, should the Board consider there is an incident that meets the conditions for consideration through a review, then the Board would also consider preparing draft Terms of Reference for Ministerial consideration, determining initial lines of enquiry, publishing the Terms of Reference, forming the Expert Panel pool, and commencing the first cyber incident review.

3. Overview of the Board

The Board consists of a Chair and up to six standing members appointed by the Minister following a 2025 expression of interest process, in accordance with Government merit and transparency requirements.

Standing members: vote on referral acceptance and final recommendations and actively participate in incident reviews by leading lines of inquiry and contributing to the assimilation, evaluation and reporting of data in relation to the cyber incident review.

Board membership

Chair

s. 22(1)(a)(ii)

Standing members

s. 22(1)(a)(ii)

Appointment of Expert Panel

The Board will be supported by an Expert Panel drawn from industry leaders, technical specialists, academics and practitioners, appointed through a transparent, merit-based process. This model enables the Board to access the right expertise for each incident while maintaining consistent, robust governance.

Secretariat support

The secretariat will support the Board by managing all administrative functions, including scheduling, document control, secure communication, minute-taking, and tracking action items. The secretariat will also provide policy, analytical and drafting support to assist the Board in undertaking its reviews and preparing draft reports, noting that all decisions and final content remain a matter for the Board.

Secretariat Contact information

Name	Role	Contact
s. 22(1)(a)(ii)	Director, secretariat	s. 22(1)(a)(ii) @homeaffairs.gov.au m: s. 22(1)(a)(ii)
s. 22(1)(a)(ii)	A/g Assistant Director secretariat	s. 22(1)(a)(ii) @homeaffairs.gov.au m: s. 22(1)(a)(ii)
s. 22(1)(a)(ii)	Policy Officer secretariat	s. 22(1)(a)(ii) @homeaffairs.gov.au m: s. 22(1)(a)(ii)
Cyber Incident Review Board Mailbox		CIRB.Enquiries@homeaffairs.gov.au

4. Overview of the Board mission and strategic priorities

The Board's core mission is to conduct expert, no-fault reviews of significant cyber security incidents in Australia. Through these reviews, the Board will identify lessons learned and develop system wide recommendations to strengthen national cyber resilience. Each review will culminate in a publicly available report that provides government, industry and the community with practical insights to support improved prevention, detection, response and recovery for future incidents of a similar nature.

Under the *Cyber Security Act 2025* (Cth), (the Act) the Board is empowered to request information from entities involved in an incident under review. Where voluntary cooperation is not achieved, the Act provides the Board with limited compulsory information gathering powers to obtain only the information necessary to complete its review.

The Minister for Cyber Security (the Minister) is responsible for the appointment and dismissal of the Chair and standing members. The Minister also approves the Terms of Reference for each review. Any amendments the Board proposes to the Terms of Reference must be submitted to, and approved by, the Minister.

Beyond these statutory touchpoints, the Board operates as an independent statutory body. In performing its functions, it is not subject to direction from any person or body, including the Minister.

4.1. Recommended initial engagements

To support early momentum and establish strong foundations for the Board's work, we recommend you undertake a series of engagements with key stakeholders across Government, within your first month.

This could include engagements with senior officials from Department of Home Affairs, the National Office of Cyber Security and the Australian Signals Directorate. The secretariat will work with you and relevant offices to prioritise and schedule these engagements.

4.2. Legislative and governance responsibilities

The Board is established under Part 5 of the *Cyber Security Act 2024* (the Act). Under section 60 of the Act, the Board is an independent statutory advisory body whose functions are to cause reviews to be conducted by review panels in relation to cyber security incidents or series of cyber security incidents.

The Board also has legislative obligations in respect to the subordinate legislation, the *Cyber Security (Cyber Incident Review Board) Rules 2025*.

4.3. Role and responsibilities of the Chair

As Chair, you are responsible for leading the effective functioning of the Board and exercising the powers provided under the Act and associated Rules. In this capacity, you will:

- Convene and preside over Board meetings, ensuring deliberations are orderly, well-formed and directed toward the Board's statutory purpose.

- Request, and where necessary require, information from entities involved in an incident under review, using the Board's limited compulsory information-gathering powers when voluntary cooperation is not achieved.
- Determine whether information provided to the Board is sensitive, in consultation with the entity that supplied it, and ensure appropriate handling and protection of such information.
- Determine remuneration and allowances for the Expert Panel member through the making of a legislative instrument, consistent with the framework established by the Act.
- Certify a person's involvement in a review, where required for statutory or administrative purposes.
- Ensure that the Board reviews do not interfere with ongoing criminal or civil proceedings, including by managing the timing, scope and handling of information.
- Grant leaves of absence to other Board members, ensuring continuity of Board operations.
- Revoke or terminate the appointment of an Expert Panel member in accordance with sections 24(7) and 27 of the Rules.

4.4. Remuneration

The remuneration, terms and conditions for the Chair position are set out in the *Remuneration Tribunal (Remuneration and Allowances for Holders of Part-Time Public Office) Determination 2025*.

Remuneration Tribunal determinations can be found at www.remtribunal.gov.au.

The daily fee model (see table below) provides flexibility to respond to a rapidly evolving cyber threat landscape, where the frequency and scale of incidents cannot be reliably anticipated.

Remuneration payment

	Daily Fee:	Travel Tier:
Chair	\$1,271	Travel Tier 2.
Cyber Incident Review Board		Part 3 of the <i>Remuneration Tribunal (Official Travel) Determination 2025</i> provides that Tier 2 office holders are entitled to: • Economy class air travel between Sydney, Melbourne and Canberra; and • Business class air travel for all other domestic routes. Members may elect to travel at a lower class where appropriate.

4.5. Suggested timing and approach to Board meetings

Timeline and key deliverables

Timeline							
	Month 1 Phase 1	Month 2	Month 3 Phase 2	Month 4	Month 5	Month 6 Phase 3	Phase 4
Chair	Establish Focus & Direction Stakeholder engagement	Prepare TOR Submission to MD for approval	Initial incident enquiries Scoping	Scope additional Lines of enquiry if required Lessons learned for CIRB			
Decision Points	Board Meeting 1 → Approve governance documents Establish review panel recruitment process	Board Meeting Scoping, Board & open Source (2 Weeks)	Board Meeting Finalise review scoping	Board Meeting Primary Lines of Enquiry	Board Meeting Scope additional Lines of enquiry if required	Board Meeting	Board Meeting
Enquiry Timeline	Receive referral Establish non-interference	Terms of Reference published, review commences Establish lines of enquiry	Establish lines of enquiry	Enquiry phase	Finalise enquiry phase Fact Finding Summary		Review report(s) published
Review Panel	Recruit Expert Panel	Panel complete contracts and on-boarded	Panel conduct interviews	Panel conduct interviews	Review Draft Report	Submit draft report to MD for approval	Expert panel stand down
Secretariat	Schedule meetings, agendas and onboard briefings/orientation	Schedule de-conflict meetings with stakeholders to confirm investigation and response finalised	Assist Board gathering and analysing information	Assist Board with drafting material	Draft fact finding Summary	Archive enquiry records	Disseminate Report to key stakeholders Draft lessons learned documentation

Figure 2. 6 month timeline and key deliverables

4.5.1. Meetings

The Board will hold meetings, as required, for the conduct of reviews and other matters. The Chair must preside at all meetings. If the Chair is unable to preside, the other standing members of the Board must appoint a standing member to preside.

The Chair may convene a Board meeting at any time and where possible, Board members will receive a minimum seven days' notice of a Board meeting. The Chair must convene a meeting within 30 days after receiving a written request to do so from another Board member. *[Note: Timeframes are subject the agreement of the Board and are not required by the Act or the Rules]*

Meetings and attendance

The Board is expected to conduct most of its work virtually. In-person attendance will only be required where briefings classified at SECRET or above are necessary for the conduct of a review.

Estimated meetings of the Board and out-of-session commitments

While the Board has broad discretion to determine its operating arrangements, departmental modelling, drawing on investigation methodologies and lessons from previous independent reviews, provides an indicative outline of the likely number of Board meetings and associated out-of-session commitments.

Out-of-session responsibilities and time commitments

Board members will be expected to undertake reasonable preparation outside formal meetings, including reviewing briefing materials, agendas and supporting documentation prepared by the secretariat.

Out-of-session responsibilities may also include contributing to the recruitment of Expert Panel members and engaging with incident stakeholders when information is requested during a review.

Members serving on a review panel may be required to participate in virtual or in-person engagements with entities affected by an incident or providing information to the review. Based on modelling of affected entities and relevant stakeholder groups, it is estimated a review panel will engage with approximately eight entities during a single review. Attendance at these sessions will be targeted – not all Board members will be required for every engagement.

5. The Expert Panel

Roles and responsibilities of the Expert Panel

The Department will support the Board to establish the Expert Panel to support reviews.

Once appointed by the Chair, the Board may draw on the Expert Panel to support individual reviews. Use of the Expert Panel is entirely at the discretion of the Board.

The Board may also commence a cyber incident review without an Expert Panel in place. For each review, the Board may establish a review panel by selecting individuals from a pool of candidates assessed against eligibility criteria and a skills matrix relevant to the specific review.

5.1.1. Eligibility and recruitment process

Eligibility for appointment to the Board and Expert Panel is established in the Rules. Members of the Board or Expert Panel are not expected to have all the identified skills and experience. However, they must demonstrate 'significant' experience or qualifications in one or more of the listed skills.

To meet the criteria for appointment, a person is required to score a '4' against one or more of the eligibility criteria.

Members of the Panel must be eligible to hold an Australian Government security clearance or equivalent clearance recognised by the Government, which assesses an individual as eligible to handle material classified up to and including SECRET.

The Department has an ongoing expression of interest submission form on the Home Affairs website, and also received expressions of interest for the Expert Panel during the recent Board recruitment process. The Board may use this repository to source membership to the Expert Panel.

All candidates for the Expert Panel are required to submit a conflict-of-interest declaration, any changes to which must be logged in the conflict-of-interest register kept by the Board.

5.1.2. Remuneration of Expert Panel

An appointment to the Expert Panel is on a part-time basis; the office of the member of the Expert Panel is not a public officer within the meaning of the *Remuneration Tribunal Act 1973* (Cth).

Expert Panel members will be paid the remuneration and allowances determined by the Chair of the Board.

The amount of remuneration will be informed by what other individuals receive performing similar or equivalent functions within Government and industry.

6. Key Stakeholders and Contacts

The Board has strategic alignment and public accountability with the Department and will engage with a range of government, regulatory, industry and community stakeholders. These stakeholders are primarily Government agencies and regulators, industry and peak bodies, as well as the entities relevant to reviews undertaken by the Board.

Key stakeholders include the Australian Federal Police, the National Office of Cyber Security and the Australian Signals Directorate. The Chair plays an important role in establishing and maintaining relationships with the Board's key stakeholders and other parties of interest.

The secretariat will provide briefing materials and governance guidance throughout the review process.

At the commencement of your term as Chair, the secretariat will work with you to facilitate initial meetings with key stakeholders.

7. Draft Governance Documents

The secretariat has prepared the following key draft governance documents for the Board to consider, which will be provided separately in a follow-up email for your consideration:

Cyber Incident Review Board Charter

The Charter sets out the functions, constitution and operation of the Board, and outlines operational matters to ensure the Board can function effectively and meet its responsibilities under the Act.

Code of Conduct

Board members adhere to the Cyber Incident Review Board Code of Conduct and agree to comply with the Code of Conduct for the term of their appointment.

Conflict of Interest Policy

In accordance with the Act, statutory officers must disclose and take reasonable steps to avoid any conflict of interest (real or perceived), in connection with their duties as office holder.

No Fault Policy Framework

Provides guidance on the legislative obligations for the Board with regards to conducting a review without apportioning blame on affected entities, and outlines the voluntary nature for entities to provide information, as required, while the Board is reviewing a cyber security incident.

8. Information Storage and Access Controls

Under the Board, the review panel is not authorised to record, use, or disclose information to the extent that such actions are prohibited or restricted under the *Privacy Act 1988* (PA). The review panel will ensure sensitive information is appropriately protected, while maintaining the ability to share lessons learned and rely on existing information-handling protections under the *Public Service Act 1999* (Cth), the *Intelligence Services Act 2001* (Cth), and the *Public Governance, Performance and Accountability Act 2013* (Cth). Persons engaged in the Review who are not otherwise bound by these legislative requirements will be contracted under equivalent confidentiality and information-protection provisions.

The secretariat manages the secure storage and access of information submitted to the Board. All information will be stored in the Department's approved information management system (Content Manager), with access limited to the Chair and the Secretariat.

8.1.1. Data Usage

Cyber incident review data provided by a reporting entity or collected by the Board during a review is protected and can only be used for the purposes of the review – it may not be used or shared for enforcement actions.

Version number	Date of issue	Author(s)	Brief description of change
0.1	20/02/2026	s. 22(1)(a)(ii)	Draft Document Created
0.2	17/04/2026	s. 22(1)(a)(ii)	Approved.



Cyber Incident Review Board Appointment Information Pack

Congratulations on your appointment as a standing member to the Cyber Incident Review Board (the Board).

This Appointment Information Pack provides key information to support your commencement, and outlines the Board's purpose, structure and operational arrangements.

The *Cyber Security Act 2024* (Cth) (the Act) establishes the Board as an independent statutory advisory body responsible for conducting no-fault, post-incident reviews of significant cyber security incidents in Australia. The Board will make recommendations to Government and industry on actions that could strengthen national preparedness, improve detection and response, and minimise the impact of similar incidents in the future.

The Board comprises a Chair and standing members, and will appoint the Expert Panel to support reviews. The Board is supported by a dedicated secretariat within the Department of Home Affairs (the Department).

The secretariat will contact you shortly with further information on the Board's commencement.

Board membership

Chair

s. 22(1)(a)(ii)

Standing members

s. 22(1)(a)(ii)

Appointment of Expert Panel

The Department will support the Board to establish the Expert Panel to support reviews. Once appointed by the Chair, the Board may draw from the Panel to support individual reviews. Use of the Expert Panel is entirely at the discretion of the Board.

Appointment of the Expert Panel is not required for the Board to commence a review.

Australian Government Security Clearance

Members of the Board, including the Expert Panel, are required to hold an Australian Government Negative Vetting 1 (NV1) security clearance to participate in the Board's governance and review activities.

The Board's work involves access to sensitive information relating to significant cyber security incidents. This information may include operational details, threat intelligence, vulnerabilities, and information about government or industry systems which are classified for national security or commercial-in-confidence reasons.

An NV1 clearance ensures an individual has been assessed as eligible to handle material classified up to and including SECRET, and as such fully participate in all aspects of the Board's work.

The Department will sponsor and support any member who does not currently hold an Australian Government security clearance to obtain an NV1 clearance.

Conflict of interest declaration

The *Cyber Security (Cyber Incident Review Board) Rules 2025* set clear requirements for managing conflicts of interest before and during appointment. Prior to appointment, members must disclose all relevant pecuniary and non-pecuniary interests.

After appointment, members must disclose interests to the Minister in accordance with section 29 of the *Public Governance, Performance and Accountability Act 2013* (Cth) and associated rules. The Board will maintain systems for integrity, risk oversight and internal control, and take reasonable steps to prevent, identify and manage conflicts of interest.

In line with the Act, statutory officers must disclose and take reasonable steps to avoid any real or perceived conflicts of interest in performing their duties.

Standing member remuneration

Sections 65 and 67 of the Act provide that standing members are remunerated as determined by the Remuneration Tribunal.

Under the *Remuneration Tribunal (Remuneration and Allowances for Holders of Part-time Public Office) Determination 2025*, standing members are remunerated as Part-time Public Office Holders using a daily fee model.

The daily fee model (see table below) provides flexibility to respond to a rapidly evolving cyber threat landscape, where the frequency and scale of incidents cannot be reliably anticipated.

Remuneration payment

	Daily Fee:	Travel Tier:
Standing Member	\$995	Travel Tier 2
Cyber Incident Review Board		Part 3 of the Remuneration Tribunal (Official Travel) Determination 2025 provides that Tier 2 office holders are entitled to: • Economy class air travel between Sydney, Melbourne and Canberra; and • Business class air travel for all other domestic routes. Members may elect to travel at a lower class where appropriate.

Meetings and attendance

The Board is expected to conduct most of its work virtually. In-person attendance will only be required where briefings classified at SECRET or above are necessary for the conduct of a review.

Estimated meetings of the Board and out-of-session commitments

While the Board has broad discretion to determine its operating arrangements, departmental modelling, drawing on investigation methodologies and lessons from previous independent reviews, provides an indicative outline of the likely number of Board meetings and associated out-of-session commitments.

Out-of-session responsibilities and time commitments

Board members will be expected to undertake reasonable preparation outside formal meetings, including reviewing briefing materials, agendas and supporting documentation prepared by the secretariat. Out of session responsibilities may also include contributing to the recruitment of Expert Panel members and engaging with incident stakeholders when information is requested during a review.

Members serving on a review panel may be required to participate in virtual or in-person engagements with entities affected by an incident or providing information to the review. Based on modelling of affected entities and relevant stakeholder groups, it is estimated a review panel will engage with approximately 8 entities during a single review. Attendance at these sessions will be targeted – not all Board members will be required for every engagement.

Governance – next steps

Once established, the Board will determine its operating and governance arrangements. Standing Members may be asked to participate in, or lead, committees supporting areas such as risk and assurance, Expert Panel appointments, and stakeholder engagement.

The secretariat will work with the Chair to convene the inaugural governance meeting, where operating procedures, committee structures and early review priorities will be confirmed. Standing Members will play a key role in shaping these foundations

The Chair may convene a meeting at any time. Where possible, members will receive at least 7 days' notice. The Chair must convene a meeting within 30 days of receiving a written request from another member.

Secretariat

The secretariat will support the Board by managing all administrative functions, including scheduling, document control, secure communication, minute-taking and tracking action items. The secretariat will also provide policy, analytical and drafting support to assist the Board in undertaking its reviews and preparing draft reports, noting that all decisions and final content remain a matter for the Board.

Secretariat Contact information

Name	Role	Contact
s. 22(1)(a)(ii)	Director, secretariat	s. 22(1)(a)(ii) @homeaffairs.gov.au m: s. 22(1)(a)(ii)
s. 22(1)(a)(ii)	A/g Assistant Director, secretariat	s. 22(1)(a)(ii) @homeaffairs.gov.au m: s. 22(1)(a)(ii)
s. 22(1)(a)(ii)	Policy Officer, secretariat	s. 22(1)(a)(ii) @homeaffairs.gov.au m: s. 22(1)(a)(ii)
Cyber Incident Review Board Mailbox		CIRB.Enquiries@homeaffairs.gov.au

~~PROTECTED CABINET~~

ASSISTANT MINISTER TO THE PRIME MINISTER
 ASSISTANT MINISTER FOR THE PUBLIC SERVICE
 ASSISTANT MINISTER FOR EMPLOYMENT AND WORKPLACE RELATIONS
 MEMBER FOR PERTH
 The Hon Patrick Gorman MP

Reference: MC26-041682

The Hon Tony Burke MP
 Minister for Home Affairs
 Minister for Immigration and Citizenship
 Minister for Cyber Security
 Minister for the Arts
 Parliament House
 CANBERRA ACT 2600

Dear Minister

Thank you for your letter dated 20 March 2026 to the Hon Anthony Albanese MP, Prime Minister, regarding the appointment of members to the inaugural Cyber Incident Review Board (the Board). The Prime Minister has asked me to reply on his behalf.

The Board will play an important role in improving Australia's resilience to growing cyber security threats through independent, no-fault post-incident reviews of nationally significant cyber incidents. I acknowledge that reviews undertaken by the Board will make recommendations to Government and industry about actions that could be taken to prevent, detect, respond to, or minimise the impact of future cyber security incidents of a similar nature. I note the Board will conduct reviews in accordance with Part 5 of the *Cyber Security Act 2024* and the Cyber Security (Cyber Incident Review Board) Rules 2025.

I approve the appointment of s. 22(1)(a)(ii) and s. 22(1)(a)(ii) as standing members of the Board for a maximum period of four years, commencing in May 2026. I note your advice that Board nominees are both relevantly experienced and representative of women, culturally and linguistically diverse persons, and geographic location. Additionally, I note that through the assessment process, all nominees have provided Private Interests Declaration forms, including mitigation strategies where potential or actual conflicts of interest might arise.

For appointments made before 2 February 2026, the Australian Public Service (APS) Commission's Merit and Transparency policy (Merit-based selection of APS agency heads and APS statutory office holders) required an open and merit-based assessment of nominees to be undertaken. On 2 September 2025, I agreed to your request for an exemption for a full merit-based recruitment process for board appointments, given that appointments would only be on a part-time basis. I note that your proposed appointees have been identified through an expression of interest process, that aligns with the open and merit-based principles.

Parliament House CANBERRA ACT 2600

~~PROTECTED CABINET~~

Released by Department of Home Affairs
 under the Freedom of Information Act 1982

~~PROTECTED CABINET~~

In future, should you intend to appoint any full-time board members, I ask that you conduct a full merit-based recruitment process in line with the new Australian Government Appointments Framework.

I ask that you work with the Prime Minister's Office on the details for the announcement of the membership for the Board, including the timing of any announcements.

I have copied this letter to the Prime Minister.

Yours sincerely



PATRICK GORMAN

16/04/2026

Released by Department of Home Affairs
under the Freedom of Information Act 1982

~~PROTECTED CABINET~~