FACTSHEET

Cyber Incident Review Board

Cyber Security Act 2024 – Part 5

The *Cyber Security Act 2024* establishes the Cyber Incident Review Board (the Board) as an **independent statutory advisory body** to conduct no-fault, post-incident reviews of significant cyber security incidents in Australia and make recommendations to Government and industry about actions that could be taken to prevent, detect, respond to, or minimise the impact of cyber security incidents of a similar nature in the future.

Composition of Board

The Board will be comprised of a **Chair, Standing Members**, an **Expert Panel**, and will be supported by staff from the Department of Home Affairs.

The **Expert Panel will be a pool of persons** comprised of industry participants, subject matter experts, cyber security specialists, academics, and other individuals as appointed to assist the Board to undertake a review of a cyber security incident.

Board members, including the Chair and Standing Members, will be appointed for **a maximum term of 4 years**, and must disclose all interests, pecuniary or otherwise, that they may have in relation to the Board or its equities.

The **Minister for Cyber Security** will:

- have oversight of appointments and dismissals of the Chair and standing members of the Board;
- establish governance parameters for the Board through subordinate legislation; and
- approve Terms of Reference for individual reviews.

The Minister for Cyber Security will appoint the Chair and Standing Members of the Board.

The Board may appoint one or more members of the Expert Panel to assist it (the Board) to undertake a Review.

Reviews undertaken by the Board

Each review will be conducted by a review panel that consists of the Chair of the Board, the Standing Members and one or more members of the Expert Panel, who will be allocated based on their qualifications, knowledge, skills or experience in relation to the particular review.

- Should the Chair or a Standing Members of the Board have a conflict of interest with a review, that person may be ineligible to participate in that review and the decision recorded in the minutes of the Board for transparency.

The Board may conduct a review in relation to a significant cyber security incident on written referral by either the Minister for Cyber Security, the National Cyber Security Coordinator, an impacted entity, or a member of the Board.

A review may **only** be conducted **after the cyber security incident or series of incidents has occurred,** and the immediate response has ended; the Minister has approved the Terms of Reference and where the incident or series of incidents:

- has seriously prejudiced the social or economic stability of Australia or it's people, the defence of Australia or national security;
- has involved novel or complex methods or technologies; or
- could reasonably be of serious concern to the Australian people.

To support the review, the Board may seek relevant information voluntarily from entities involved in the cyber security incident. Where voluntary requests have been unsuccessful, the Chair of the Board will be enabled with **limited information gathering powers** to compel relevant information from entities involved in the cyber security incident under review.

- Where information is compelled, an entity is entitled to be paid reasonable compensation if the Chair requires them to make and produce copies of relevant documents.
- An entity may be liable to a civil penalty if it fails to comply with a notice to produce documents.

The Board must **prepare both a draft and final report** detailing its findings and recommendations.

The Board must give the draft report to the Minister, and may give the draft report, or an extract of the report to any other Commonwealth or State body or entity for the purposes of providing an opportunity to make submissions or determining whether information is sensitive review information.

In preparing the final report, the Board must consider any submissions received in relation to the draft report. The final report:

- must set out a summary of the information and material on which the findings and recommendations are based, the reasons for the recommendations, any information required by the Terms of Reference, information (if any) prescribed by the rules, and any other information that the Board considers appropriate.
- must not apportion blame, provide means to determine the liability of an entity in relation to a cyber security incident, identify an individual (unless they have consented), or allow any adverse inference to be drawn from the fact that an entity is the subject of the review.
- must redact information if the Chair is satisfied that the information is sensitive review information.

If information is redacted, the Board must prepare a protected report that includes the information and reasons for redacting the information, to be provided to the Minister and Prime Minister

Proposed Rules to establish the Board

The Rules will establish the governance parameters through which the Board will perform its functions and provide flexibility to the Board so that it can respond effectively, as technology evolves and in response to the evolving cyber threat landscape.

Each Review will be supported by a **Terms of Reference** to be drafted and established by the Board. The Rules will outline the minimum requirements that must be included in each set of Terms of Reference. Ministerial approval is required as an appropriate accountability mechanism.

The Rules will establish the requirements for **eligibility for appointment to the Board and the Expert Panel**.

- The Board and Expert Panel will share a set of common eligibility criteria, 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.

The Standing Board and Expert Panel members will be required to disclose all interests, pecuniary or otherwise, they may have in relation to the Board or its equities.

Remuneration, including allowances, for the Chair and standing members of the Board will be paid in line with the amount determined by the Remuneration Tribunal.

- Government employees appointed by the Minister as Standing Board members, or members of the Expert Panel, will not receive remuneration where their participation is connected to their permanent role within government for which they are remunerated for.
- Expert Panel members appointed to a review panel 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.

The Rules propose to establish the frameworks through which a member of the Board or Expert Panel may **resign** and powers for the Minister to **terminate the appointment** of Board Members.

- The power to terminate the appointment of a member of the Expert Panel will reside with the Chair.
- The Chair will also have the ability to revoke the appointment of a member of the Expert Panel to the review panel for a review.

Operation

Cyber Incident Review Board

- **Chair** — *Appointed by the Minister*
- **Standing Members** — *Appointed by the Minister.*
- Department of Home Affairs support staff

Expert Panel

Pool that can be called upon for individual reviews.

Industry experts with high levels of cyber security, legal or sectoral expertise and experience.

Untitled* Review**: Cyber Incident Review Board + **Expert Panel Members** — ***1 or more selected *from Expert Panel*

Review Process

1. Incident or series of incidents occur
2. Incident referred (by Minister, Board or entity)
3. Board decision to undertake review
4. Board drafts Terms of Reference, selects expert panel members
5. Minister endorses TORs
6. **Review undertaken**
   - Board may request information voluntarily
   - Board may request entity provides certain documents
   - Board considers and identifies recommendations
7. Board draft report
8. **Optional**: Consultation (Part or Full Draft Report), with Entity, Cwth State/Commercial Entities
9. Board may produce protected report
10. Board publishes final review report

The information contained in this document is general in nature and does not constitute legal advice. Readers are encouraged to obtain legal advice that applies to their particular circumstances. The Commonwealth of Australia does not guarantee the accuracy, currency or completeness of any information in this document.