Australian Government

Department of Home Affairs

Cyber Security Legislative Reforms – Explanatory Document

Cyber Security (Cyber Incident Review Board) Rules

Contact us

Enquiries regarding the licence and any use of this document are welcome at:

Department of Home Affairs
PO Box 25
BELCONNEN ACT 2616

P-23-02503-c

Contents

Cyber Incident Review Board

Cyber Incident Review Board

The *Cyber Security Act 2024* (*Cyber Security Act*) 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.

The Board will play a key role in uplifting the cyber security and national resilience of Australia by supporting the Australian Government to review and assess significant cyber incidents 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.

The Board will be comprised of a Chair, and two to six Standing Members, and will be supported by staff from the Department of Home Affairs. The Board may also establish an Expert Panel to assist the Board in the conduct of a review.

Each review will be conducted by a Review Panel that consists of the Chair of the Board, the Standing Members that are specified in the Terms of Reference for the review and one or more members of the Expert Panel appointed to assist in relation to the review. The Board will appoint individuals from the Expert Panel to the Review Panel based upon the qualifications, knowledge, skills or experience required for a particular review.

To support implementation of the CIRB framework, the Cyber Security Act enables the Minister to establish rules that outline the governance parameters ('CIRB Rules') through which the Board will perform its functions, including: procedures for reviews, common eligibility criteria for standing members and the Expert Panel, appointments of standing members and the Expert Panel and other administrative matters that will support the operations of the Board.

Division 2 - Reviews by the Board

The Board may conduct a review in relation to a 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 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 its people, the defence of Australia or national security; or
- has involved novel or complex methods or technologies; or
- could reasonably be of serious concern to the Australian people.

Upon referral, the decision to undertake a review is at the discretion of the Board, subject to the cyber security incident or series of incidents satisfying at least one of the criteria set out at subsection 46(3) of the *Cyber Security Act*.

While the Board will have discretion when deciding to undertake a review, the CIRB Rules define a set of matters they must consider when prioritising referrals and reviews. For this purpose, the Board must have regard to:

- the severity and scale of impact of the cyber security incident, or incidents, to which the referral or review relates, as established in s46(2) of the Cyber Security Act;
- the availability and capacity of standing members of the Board;
- the availability and capacity of members of the Expert Panel;
- the relevance of skills, knowledge or experience of members of the Expert Panel to assist in undertaking a review.

Should the Board be satisfied that a cyber-incident meets the criteria in the Act and that a review should be conducted, it must establish Terms of Reference. The Terms of Reference will be drafted by the Board for approval by the Minister for Cyber Security. In line with the Board's independent function, the Board will have discretion in drafting the Terms of Reference—including the scope of the review and how the Board will work with key stakeholders to conduct the review, amongst other matters. However, the CIRB Rules provide that the Terms of Reference must include certain details on elements of the review such as:

- the number of standing members of the Board who will conduct the review and the number of members of the Expert Panel to be appointed to assist the Board in relation to the review;
- the minimum Australian Government security clearance, or equivalent security clearance recognised by the Commonwealth, required for a standing member of the Board to hold in order to participate in the conduct of the review; and
- any eligibility requirements, additional to those set out in the CIRB Rules, for the appointment of members of the Expert Panel to assist the Board in relation to the review. For example, these may relate to particular skills, qualifications, expertise or experience that relate to the cyber security incident being reviewed.

During the course of a review, circumstances may rise that give cause to amending the Terms of Reference. For example, the Board may identify certain issues during its information gathering phase that should be reviewed but that are not within scope of the existing Terms of Reference. To ensure there is an ability to amend the scope of the review, the CIRB Rules allow the Board to vary the Terms of Reference with the approval of the Minister for Cyber Security.

Following a decision to conduct a review, the CIRB Rules require the Board must publish as soon as practicable a notice that a review will be conducted. The notice is to be published on the Department's website or in any other way the Board considers appropriate. The notification must include:

- the number of standing members of the Board who will conduct the review and the number of the Expert Panel members to be appointed to assist in the conduct of the review;
- details of the cyber security incident, or series of cyber security incidents, that will be subject of the review;
- a brief description of how the incident or series of incidents meets the requirements in s46(2) of the Cyber Security Act;
- proposed timeframes for the conduct of the review; and
- any other information the Board considers appropriate.

Division 3 – Standing Members of the Board

Subsection 66(4) and 69(1) of the *Cyber Security Act* provide the Minister for Cyber Security with the ability to establish rules in relation to the standing members of the Board, including the eligibility for appointment as a standing member and the terms and conditions of that appointment. In accordance with the Parliamentary Joint Committee on Intelligence and Security Advisory Report into the Cyber Security Legislative Package, consultation on the Rules will inform the composition of the standing members of the Board, including whether membership is extended to both government and non-government personnel.

It is proposed that standing members and the Expert Panel share a common eligibility criteria. The Minister and the Chair will consider appointment of Board Members and the Expert Panel in accordance with the legislative framework and through a skills matrix that seeks to ensure an appropriate mix of skills and experience are available for a Review Panel. Recognising standing members form a core component of the Board, it is proposed that individuals appointed have strong leadership and strategic experience in addition to the eligibility criteria in the CIRB Rules.

The CIRB Rules provide that the Minister may appoint a person as a standing member of the Board where they are satisfied that the person meets prescribed the eligibility requirements, including:

- the person holds or be eligible to hold a Commonwealth security clearance or equivalent clearance recognised by the Commonwealth, which allows access to information of at least secret, **and**
- the person has qualifications and significant experience in the field of law, qualifications or significant experience in the field of cyber security or information security, significant experience in incident management or crisis response, audit, assurance or review processes, public administration or financial or prudential regulation, critical infrastructure sector (within the meaning of the *Security of Critical Infrastructure Act 2018*), or significant academic qualifications or knowledge in a relevant field, **or**
- the person holds a relevant Commonwealth, State or Territory government position at an appropriately senior level.[1]

The CIRB Rules provides the Minister for Cyber Security with the ability to appoint a person to act as a standing member of the Board, including in circumstances when a standing member is absent or otherwise unable to fulfil their duties. A person appointed to act as a standing member of the Board must meet the eligibility criteria outlined in the Rules. In accordance with section 68 of the Cyber Security Act, the Minister for Cyber Security may also appoint a standing member of the Board to act as the Chair.

It is essential to the integrity of the Board that any perceived or actual conflicts of interests in the Board, its interests or equities are identified and managed. The Board will establish and maintain appropriate systems of integrity and risk oversight, management and internal control, and will take all reasonable measures to prevent, detect and deal with conflict of interests.

The CIRB Rules articulate clear parameters and expectations for managing conflicts of interests before and during appointment to the Board. Relevantly, the CIRB Rules require that before the Minister appoints a Board member, the proposed member must disclose all interests, pecuniary or otherwise, that the person is aware of having in a matter of a kind likely to be considered by the Board. Disclosures after appointment must be made to the Minister in accordance with section 29 of the Public Governance, Performance and Accountability Act 2013 and any rules made for the purposes of section 29 of the Public Governance, Performance and Accountability Act 2013.

Once appointed to the Board, the CIRB Rules require a Board member to disclose to the Board, as soon as possible after the relevant facts have come to the Board member's knowledge, any interest in a matter which is being or about to be considered by the Board in relation to a review. To ensure transparency, the disclosure must be recorded in the minutes of a meeting of the Board. The Board member must not be present or take part in any deliberation or decision by the Board in relation to the matter, unless the Board determines otherwise.

To maintain the Board's integrity, the CIRB Rules also restrict Board members from engaging in any paid work, which in the Minister's opinion, conflicts or could conflict with the proper performance of the Board Member's duties.

The CIRB Rules enable the Minister to determine the conditions for any leave of absence for the Chair, with the Chair, in turn, determining the conditions for leave of absence for Board members. Where a Board member is absent for more than three

[1] Participation of State and Territory Government officials will only occur with the agreement of the State and Territory concerned.

consecutive months, the Chair must notify the Minister, so that the Minister may consider if acting appointments are required in that time.

The CIRB Rules also enable Board members to resign from the Board in writing to the Minister and outline the circumstances and processes in which the Minister may terminate members of the Board, including members of the Expert Panel, these include but are not limited to:

- misbehaviour;
- if the Board or Expert Panel member is unable to fulfil their duties due to physical or mental incapacity;
- if the Board or Expert Panel member becomes bankrupt, or applies to take the benefit of any law for the relief of bankrupt or insolvent debtors;
- if the Board member is absent, except for a leave of absence, for 3 or more consecutive meetings;
- if the Board member engages in paid work which the Minister is of the opinion that it would interfere with the proper performance of their duties[2]; or
- if the Board or Expert Panel member does not comply with disclosure requirements specified in the rules.

Division 4 – Expert Panel

The CIRB Rules enable the Chair of the Board to appoint a person to the Expert Panel on a part time basis. The appointment must not exceed four years. It is the intention that the Expert Panel is 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. The members will be called upon to assist the Board with a review through their inclusion in the Terms of Reference.

Persons must meet the eligibility criteria in the CIRB Rules to be eligible to be appointed as a member of the Expert Panel. A person is only eligible to be appointed as a member of the Expert Panel if the person:

- holds or is eligible to hold a Commonwealth security clearance or equivalent clearance recognised by the Commonwealth, which allows access to information of at least secret; **and**
- the person has qualifications and significant experience in the field of law, qualifications in the field of cyber security, information technology, computer networks or software engineering or significant experience in cyber security, information security, incident management, crisis response, audit, assurance or review processes, public administration or financial or prudential regulation, critical infrastructure sector (within the meaning of the *Security of Critical Infrastructure Act 2018*), or significant academic qualifications or knowledge in a relevant field; or
- the person holds a relevant Commonwealth, State or Territory government position at an appropriately senior level.

To ensure the Board has national representation, the CIRB Rules enable the Chair to appoint a State or Territory government employee to the Expert Panel, but only with the agreement of the State or Territory concerned. State and Territory representatives will need to meet the eligibility criteria prior to being appointed to the Expert Panel.

Subsection 70(3) of the Cyber Security Act enables the Board to appoint one or more members of the Expert Panel to the Review Panel to assist the Board to undertake a review of a significant cyber incident or series of cyber incidents. The CIRB Rules outline that a member of the Expert Panel may only be appointed to a Review Panel if the Chair of the Board is satisfied of the following:

- the person meets the eligibility criteria specified in the Terms of Reference for the review;
- the member has appropriate qualifications, skills or experience to assist in the conduct of the particular review;
- the member will not be engaged in any work which conflicts with the conduct of their duties in relation to the review.

The CIRB Rules provide the framework through which a member of the Expert Panel may resign from the Expert Panel or from their appointment to a Review Panel by giving the Chair of the Board a written resignation. The CIRB Rules establishes a framework through which the Chair of the Board may revoke the appointment of a member of the Expert Panel to the Review Panel. A revocation may occur for the following reasons:

- misbehaviour; or
- if the member of the Expert Panel is unable to perform their duties due to physical or mental incapacity; or
- the member becomes bankrupt, or applies to take the benefit of any law for the relief of bankrupt or insolvent debtors, or compounds with the member's creditors, or makes an assignment of the member's remuneration for the benefit of the member's creditors; or
- the member fails to comply with disclosure requirements in the CIRB Rules; or
- the Chair is no longer satisfied that the member of the Expert Panel meets the eligibility criteria.

[2] Members of the Expert Panel will be subject to the Conflict of Interest Framework which will enable management of this risk should they be appointed to a Review Panel.

The CIRB Rules also enable the Chair to terminate the appointment of a member of the Expert Panel in certain circumstances. Termination from the Expert Panel will mean that a person is not a member of any Review Panel. Reasons for termination may include but are not limited to:

- misbehaviour;
- if the member of the Expert Panel is unable to perform their duties due to physical or mental incapacity;
- the member becomes bankrupt, or applies to take the benefit of any law for the relief of bankrupt or insolvent debtors or compounds with the member's creditors, or makes an assignment of the member's remuneration for the benefit of the member's creditors; or
- the member fails to comply with disclosure requirements in the Governance Rule; or
- the Chair is no longer satisfied that the member of the Expert Panel meets the eligibility criteria.

Consistent with the ensuring a strong integrity framework and culture within the Board, the CIRB Rules outline clear parameters and expectations for managing conflicts of interests before and during appointment to the Expert Panel.

Relevantly, before a person is appointed, they must give written notice to the Chair of the Board of all interests, pecuniary or otherwise, that conflict or could conflict with the proper performance of their duties as a member of the Expert Panel. Once appointed to the Expert Panel, the CIRB Rules require that the members must disclose to the Board, as soon as possible once they are aware of the conflict, any interest in a matter, which is being or is about to be considered by the Board.

A conflicts of interest register will be maintained for all Board members and members of the Expert Panel. This will inform the Board's consideration of who should partake in a Review Panel. Prior to finalising a Review Panel, the Board will request persons identified to update their declaration of interests, with updates required at each Review Board meeting.

Division 5 – Other matters relating to the Board

The CIRB Rules make clear that the Board has the independence and discretion to determine how it conducts its meetings. However, to provide transparency on the functioning of the Board, the CIRB Rules make provision for general administration and procedures of the Board, including:

- a requirement to convene such meetings as necessary for the efficient function of the Board;
- a requirement that the Chair must convene a meeting of the Board within 30 days of a written request to do so by another member of the Board.
- a requirement that the Chair must preside over all meetings of the Board, or if the Chair is not present, a requirement that the standing members appoint one of themselves to preside;
- parameters for voting arrangements;
- a requirement that minutes of each meeting are kept; and
- circumstances in which the board is taken to have made a decision without a formal meeting.

Remuneration

In accordance with section 65 and 67 of the *Cyber Security Act*, 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. Importantly, Government employees appointed as either standing members or members of the Expert Panel assisting the Review Panel will not receive remuneration where their participation is connected to their permanent role within government for which they receive existing remuneration.

The CIRB Rules provide that Expert Panel members appointed to a Review Panel are 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 receive performing similar or equivalent functions within Government and industry. The Department of Home Affairs has commenced work to establish the Remuneration Framework for the CIRB. Once finalised, the Remuneration Framework, including supporting legislative instruments, will be published on the Department's website to support transparency in operations.

/