Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Responding to Serious Cyber Security Incidents

Legislative Handbook

Security Critical Infrastructure Act 2018

February 2022

1300 27 25 24
enquiries@CISC.gov.au

Contents

The information in Responding to Serious Cyber Incidents Legislative Handbook is extracted from the Security of Critical Infrastructure Act 2018 and the Security Legislation Amendment (Critical Infrastructure) Act 2021 Explanatory Memorandum. The legislative handbook does not replace the original source documents that are available at aph.gov.au and on the Federal Register of Legislation.

Security of Critical Infrastructure Act 2018

Part 3A—Responding to serious cyber security incidents

Division 1—Simplified outline of this Part

35AA Simplified outline of this Part

- This Part sets up a regime for the Commonwealth to respond to serious cyber security incidents.
- If a cyber security incident has had, is having, or is likely to have, a relevant impact on a critical infrastructure asset, the Minister may, in order to respond to the incident, do any or all of the following things:
  - (a) authorise the Secretary to give information-gathering directions to a relevant entity for the asset;
  - (b) authorise the Secretary to give an action direction to a relevant entity for the asset;
  - (c) authorise the Secretary to give an intervention request to the authorised agency.
- An information-gathering direction requires the relevant entity to give information to the Secretary.
- An action direction requires the relevant entity to do, or refrain from doing, a specified act or thing.
- An intervention request is a request that the authorised agency do one or more specified acts or things in relation to the asset.

Division 2—Ministerial authorisation relating to cyber security incident

35AB Ministerial authorisation

Scope

(1) This section applies if the Minister is satisfied that:

(a) a cyber security incident:

(i) has occurred; or

(ii) is occurring; or

(iii) is imminent; and

(b) the incident has had, is having, or is likely to have, a relevant impact on a critical infrastructure asset (the ***primary asset***); and

(c) there is a material risk that the incident has seriously prejudiced, is seriously prejudicing, or is likely to seriously prejudice:

(i) the social or economic stability of Australia or its people; or

(ii) the defence of Australia; or

(iii) national security; and

(d) no existing regulatory system of the Commonwealth, a State or a Territory could be used to provide a practical and effective response to the incident.

Authorisation

(2) The Minister may, on application by the Secretary, do any or all of the following things:
  (a) authorise the Secretary to give directions to a specified entity under section 35AK that relate to the incident and the primary asset;
  (b) authorise the Secretary to give directions to a specified entity under section 35AK that relate to the incident and a specified critical infrastructure sector asset;
  (c) authorise the Secretary to give to a specified entity a specified direction under section 35AQ that relates to the incident and the primary asset;
  (d) authorise the Secretary to give to a specified entity a specified direction under section 35AQ that relates to the incident and a specified critical infrastructure sector asset;
  (e) authorise the Secretary to give a specified request under section 35AX that relates to the incident and the primary asset;
  (f) authorise the Secretary to give a specified request under section 35AX that relates to the incident and a specified critical infrastructure sector asset.

Note 1: Section 35AK deals with information gathering directions.

Note 2: Section 35AQ deals with action directions.

Note 3: Section 35AX deals with intervention requests.

(3) An authorisation under subsection (2) is to be known as a ***Ministerial authorisation***.

(4) Subsection 33(3AB) of the *Acts Interpretation Act 1901* does not apply to subsection (2) of this section.

Note: Subsection 33(3AB) of the *Acts Interpretation Act 1901* deals with specification by class.

Information gathering directions

(5) A Ministerial authorisation under paragraph (2)(a) or (b):
  (a) is generally applicable to the incident and the asset concerned; and
  (b) is to be made without reference to any specific directions.

(6) The Minister must not give a Ministerial authorisation under paragraph (2)(a) or (b) unless the Minister is satisfied that the directions that could be authorised by the Ministerial authorisation are likely to facilitate a practical and effective response to the incident.

Action directions

(7) The Minister must not give a Ministerial authorisation under paragraph (2)(c) or (d) unless the Minister is satisfied that:
  (a) the specified entity is unwilling or unable to take all reasonable steps to respond to the incident; and
  (b) the specified direction is reasonably necessary for the purposes of responding to the incident; and
  (c) the specified direction is a proportionate response to the incident; and
  (d) compliance with the specified direction is technically feasible.

Note: Section 12P provides examples of responding to a cyber security incident.

(8) In determining whether the specified direction is a proportionate response to the incident, the Minister must have regard to:
  (a) the impact of the specified direction on:
    (i) the activities carried on by the specified entity; and
    (ii) the functioning of the asset concerned; and
  (b) the consequences of compliance with the specified direction; and
  (c) such other matters (if any) as the Minister considers relevant.

(9) The Minister must not give a Ministerial authorisation under paragraph (2)(c) or (d) if the specified direction:
   (a) requires the specified entity to permit the authorised agency to do an act or thing that could be the subject of a request under section 35AX; or
   (b) requires the specified entity to take offensive cyber action against a person who is directly or indirectly responsible for the incident.

Intervention requests

(10) The Minister must not give a Ministerial authorisation under paragraph (2)(e) or (f) unless the Minister is satisfied that:
   (a) giving a Ministerial authorisation under paragraph (2)(c) or (d) would not amount to a practical and effective response to the incident; and
   (b) if there is only one relevant entity for the asset concerned—the relevant entity is unwilling or unable to take all reasonable steps to respond to the incident; and
   (c) if there are 2 or more relevant entities for the asset concerned—those entities, when considered together, are unwilling or unable to take all reasonable steps to respond to the incident; and
   (d) the specified request is reasonably necessary for the purposes of responding to the incident; and
   (e) the specified request is a proportionate response to the incident; and
   (f) compliance with the specified request is technically feasible; and
   (g) each of the acts or things specified in the specified request is an act or thing of a kind covered by section 35AC.

Note: Section 12P provides examples of responding to a cyber security incident.

(11) In determining whether the specified request is a proportionate response to the incident, the Minister must have regard to:
   (a) the impact of compliance with the specified request on the functioning of the asset concerned; and
   (b) the consequences of acts or things that would be done in compliance with the specified request; and
   (c) such other matters (if any) as the Minister considers relevant.

(12) The Minister must not give a Ministerial authorisation under paragraph (2)(e) or (f) if compliance with the specified request would involve the authorised agency taking offensive cyber action against a person who is directly or indirectly responsible for the incident.

(13) The Minister must not give a Ministerial authorisation under paragraph (2)(e) or (f) unless the Minister has obtained the agreement of:
   (a) the Prime Minister; and
   (b) the Defence Minister.

(14) An agreement under subsection (13) may be given:
   (a) orally; or
   (b) in writing.

(15) If an agreement under subsection (13) is given orally, the Prime Minister or the Defence Minister, as the case requires, must:
   (a) do both of the following:
      (i) make a written record of the agreement;
      (ii) give a copy of the written record of the agreement to the Minister; and
   (b) do so within 48 hours after the agreement is given.

Ministerial authorisation is not a legislative instrument

(16) A Ministerial authorisation is not a legislative instrument.

Other powers not limited

(17) This section does not, by implication, limit a power conferred by another provision of this Act.

35AC Kinds of acts or things that may be specified in an intervention request

For the purposes of the application of paragraph 35AB(10)(g) to a Ministerial authorisation of a request, each of the following kinds of acts or things is covered by this section:

(a) access or modify:
  (i) a computer that is, or is part of, the asset to which the Ministerial authorisation relates; or
  (ii) a computer device that is, or is part of, the asset to which the Ministerial authorisation relates;

(b) undertake an analysis of:
  (i) a computer that is, or is part of, the asset to which the Ministerial authorisation relates; or
  (ii) a computer program that is, or is part of, the asset to which the Ministerial authorisation relates; or
  (iii) computer data that is, or is part of, the asset to which the Ministerial authorisation relates; or
  (iv) a computer device that is, or is part of, the asset to which the Ministerial authorisation relates;

(c) if it is necessary to achieve the purpose mentioned in paragraph (b)—install a computer program on a computer that is, or is part of, the asset to which the Ministerial authorisation relates;

(d) access, add, restore, copy, alter or delete data held in:
  (i) a computer that is, or is part of, the asset to which the Ministerial authorisation relates; or
  (ii) a computer device that is, or is part of, the asset to which the Ministerial authorisation relates;

(e) access, restore, copy, alter or delete a computer program that is, or is part of, the asset to which the Ministerial authorisation relates;

(f) access, copy, alter or delete a computer program that is installed on a computer that is, or is part of, the asset to which the Ministerial authorisation relates;

(g) alter the functioning of:
  (i) a computer that is, or is part of, the asset to which the Ministerial authorisation relates; or
  (ii) a computer device that is, or is part of, the asset to which the Ministerial authorisation relates;

(h) remove or disconnect:
  (i) a computer; or
  (ii) a computer device;
  from a computer network that is, or is part of, the asset to which the Ministerial authorisation relates;

(i) connect or add:
  (i) a computer; or
  (ii) a computer device;
  to a computer network that is, or is part of, the asset to which the Ministerial authorisation relates;

(j) remove:
  (i) a computer that is, or is part of, the asset to which the Ministerial authorisation relates; or
  (ii) a computer device that is, or is part of, the asset to which the Ministerial authorisation relates;
  from premises.

35AD Consultation

(1) Before giving a Ministerial authorisation under paragraph 35AB(2)(c) or (d), the Minister must consult the specified entity unless the delay that would occur if the specified entity were consulted would frustrate the effectiveness of the Ministerial authorisation.

(2) Before giving a Ministerial authorisation under paragraph 35AB(2)(e) or (f) in relation to an asset, the Minister must:
   (a) if the asset is a critical infrastructure asset—consult the responsible entity for the asset; or
   (b) if the asset is a critical infrastructure sector asset (other than a critical infrastructure asset)—consult whichever of the following entities the Minister considers to be most relevant in relation to the proposed authorisation:
      (i) the owner, or each of the owners, of the asset;
      (ii) the operator, or each of the operators, of the asset;

   unless the delay that would occur if the entity or entities were consulted would frustrate the effectiveness of the Ministerial authorisation.

(3) If subsection (1) or (2) requires an entity to be consulted, that consultation must involve:
   (a) giving the entity a copy of the draft Ministerial authorisation; and
   (b) inviting the entity to make a submission to the Minister about the draft Ministerial authorisation within 24 hours after receiving the copy of the draft Ministerial authorisation.

35AE Form and notification of Ministerial authorisation

(1) A Ministerial authorisation may be given:
   (a) orally; or
   (b) in writing.

(2) The Minister must not give a Ministerial authorisation orally in relation to:
   (a) a cyber security incident; and
   (b) an asset;

   unless the delay that would occur if the Ministerial authorisation were to be made in writing would frustrate the effectiveness of:
   (c) any directions that may be given under section 35AK or 35AQ in relation to the incident and the asset; or
   (d) any requests that may be given under section 35AX in relation to the incident and the asset.

Notification of Ministerial authorisations given orally

(3) If a Ministerial authorisation is given orally in relation to:
   (a) a cyber security incident; and
   (b) an asset;

   the Minister must:
   (c) do both of the following:
      (i) make a written record of the Ministerial authorisation;
      (ii) give a copy of the written record of the Ministerial authorisation to the Secretary and the Inspector-General of Intelligence and Security; and
   (d) do so within 48 hours after the Ministerial authorisation is given.

(4) If a Ministerial authorisation is given orally in relation to:
   (a) a cyber security incident; and

(b) a critical infrastructure asset;

the Minister must:

(c) do both of the following:

(i) make a written record of the Ministerial authorisation;

(ii) give a copy of the written record of the Ministerial authorisation to the responsible entity for the asset; and

(d) do so within 48 hours after the Ministerial authorisation is given.

(5) If a Ministerial authorisation is given orally in relation to:

(a) a cyber security incident; and

(b) a critical infrastructure sector asset (other than a critical infrastructure asset);

the Minister must:

(c) make a written record of the Ministerial authorisation; and

(d) give a copy of the written record of the Ministerial authorisation to whichever of the following entities the Minister considers to be most relevant in relation to the Ministerial authorisation:

(i) the owner, or each of the owners, of the asset;

(ii) the operator, or each of the operators, of the asset; and

(e) do so within 48 hours after the Ministerial authorisation is given.

Notification of Ministerial authorisations given in writing

(6) If a Ministerial authorisation is given in writing in relation to:

(a) a cyber security incident; and

(b) an asset;

the Minister must:

(c) give a copy of the Ministerial authorisation to the Secretary and the Inspector-General of Intelligence and Security; and

(d) do so within 48 hours after the Ministerial authorisation is given.

(7) If a Ministerial authorisation is given in writing in relation to:

(a) a cyber security incident; and

(b) a critical infrastructure asset;

the Minister must:

(c) give a copy of the Ministerial authorisation to the responsible entity for the asset; and

(d) do so within 48 hours after the Ministerial authorisation is given.

(8) If a Ministerial authorisation is given in writing in relation to:

(a) a cyber security incident; and

(b) a critical infrastructure sector asset (other than a critical infrastructure asset);

the Minister must:

(c) give a copy of the Ministerial authorisation to whichever of the following entities the Minister considers to be most relevant in relation to the Ministerial authorisation:

(i) the owner, or each of the owners, of the asset;

(ii) the operator, or each of the operators, of the asset; and

(d) do so within 48 hours after the Ministerial authorisation is given.

35AF Form of application for Ministerial authorisation

(1) The Secretary may apply for a Ministerial authorisation either:

(a) orally; or
(b) in writing.

(2) The Secretary must not apply orally for a Ministerial authorisation that relates to:
(a) a cyber security incident; and
(b) an asset;
unless the delay that would occur if the application were to be made in writing would frustrate the effectiveness of:
(c) any directions that may be given under section 35AK or 35AQ in relation to the incident and the asset; or
(d) any requests that may be given under section 35AX in relation to the incident and the asset.

(3) If an application for a Ministerial authorisation is made orally, the Secretary must:
(a) do both of the following:
(i) make a written record of the application;
(ii) give a copy of the written record of the application to the Minister; and
(b) do so within 48 hours after the application is made.

35AG Duration of Ministerial authorisation

Scope

(1) This section applies if a Ministerial authorisation is given in relation to:
(a) a cyber security incident; and
(b) an asset.

Duration of Ministerial authorisation

(2) Subject to this section, the Ministerial authorisation remains in force for the period specified in the Ministerial authorisation (which must not exceed 20 days).

Fresh Ministerial authorisation

(3) If a Ministerial authorisation (the ***original Ministerial authorisation***) is in force, this Act does not prevent the Minister from giving a fresh Ministerial authorisation that:
(a) is in the same, or substantially the same, terms as the original Ministerial authorisation; and
(b) comes into force immediately after the expiry of the original Ministerial authorisation.

(4) In deciding whether to give such a fresh Ministerial authorisation, the Minister must have regard to the number of occasions on which Ministerial authorisations have been made in relation to the incident and the asset.

(5) Subsection (4) does not limit the matters to which the Minister may have regard to in deciding whether to give a fresh Ministerial authorisation.

35AH Revocation of Ministerial authorisation

Scope

(1) This section applies if a Ministerial authorisation is in force in relation to:
(a) a cyber security incident; and
(b) an asset.

Power to revoke Ministerial authorisation

(2) The Minister may, in writing, revoke the Ministerial authorisation.

Duty to revoke Ministerial authorisation

(3) If the Minister is satisfied that the Ministerial authorisation is no longer required to respond to the incident, the Minister must, in writing, revoke the Ministerial authorisation.

(4) If the Secretary is satisfied that the Ministerial authorisation is no longer required to respond to the incident, the Secretary must:
  (a) notify the Minister that the Secretary is so satisfied; and
  (b) do so soon as practicable after the Secretary becomes so satisfied.

Notification of revocation

(5) If the Ministerial authorisation is revoked, the Minister must:
  (a) give a copy of the revocation to:
    (i) the Secretary; and
    (ii) the Inspector-General of Intelligence and Security; and
    (iii) each relevant entity for the asset; and
  (b) do so within 48 hours after the Ministerial authorisation is revoked.

(6) If a Ministerial authorisation is revoked in relation to:
  (a) a cyber security incident; and
  (b) a critical infrastructure asset;
the Minister must:
  (c) give a copy of the revocation to the responsible entity for the asset; and
  (d) do so within 48 hours after the Ministerial authorisation is revoked.

(7) If a Ministerial authorisation is revoked in relation to:
  (a) a cyber security incident; and
  (b) a critical infrastructure sector asset (other than a critical infrastructure asset);
the Minister must:
  (c) give a copy of the revocation to whichever of the following entities the Minister considers to be most relevant in relation to the Ministerial authorisation:
    (i) the owner, or each of the owners, of the asset;
    (ii) the operator, or each of the operators, of the asset; and
  (d) do so within 48 hours after the Ministerial authorisation is revoked.

Revocation is not a legislative instrument

(8) A revocation of the Ministerial authorisation is not a legislative instrument.

Application of Acts Interpretation Act 1901

(9) This section does not, by implication, affect the application of subsection 33(3) of the *Acts Interpretation Act 1901* to an instrument made under a provision of this Act (other than this Part).

35AJ Minister to exercise powers personally

A power of the Minister under this Division may only be exercised by the Minister personally.

Division 3—Information gathering directions

35AK Information gathering direction

Scope

(1) This section applies if a Ministerial authorisation given under paragraph 35AB(2)(a) or (b) is in force in relation to:
  (a) a cyber security incident; and
  (b) an asset.

Direction

(2) If:
  (a) an entity is a relevant entity for the asset; and
  (b) the Secretary has reason to believe that the entity has information that may assist with determining whether a power under this Act should be exercised in relation to the incident and the asset;

the Secretary may direct the entity to:
  (c) give any such information to the Secretary; and
  (d) do so within the period, and in the manner, specified in the direction.

(3) The period specified in the direction must end at or before the end of the period for which the Ministerial authorisation is in force.

(4) The Secretary must not give the direction unless the Secretary is satisfied that:
  (a) the direction is a proportionate means of obtaining the information; and
  (b) compliance with the direction is technically feasible.

(5) The Secretary must not give a direction that would require an entity to:
  (a) do an act or thing that would be prohibited by section 7 of the *Telecommunications (Interception and Access) Act 1979*; or
  (b) do an act or thing that would be prohibited by section 108 of the *Telecommunications (Interception and Access) Act 1979*; or
  (c) do an act or thing that would (disregarding this Act) be prohibited by section 276, 277 or 278 of the *Telecommunications Act 1997*.

(6) Before giving a direction under this section to an entity, the Secretary must consult the entity unless the delay that would occur if the entity were consulted would frustrate the effectiveness of the direction.

Other powers not limited

(7) This section does not, by implication, limit a power conferred by another provision of this Act.

35AL Form of direction

(1) A direction under section 35AK may be given:
  (a) orally; or
  (b) in writing.

(2) The Secretary must not give a direction under section 35AK orally unless the delay that would occur if the direction were to be given in writing would frustrate the effectiveness of the direction.

(3) If a direction under section 35AK is given orally to an entity, the Secretary must:

(a) do both of the following:
(i) make a written record of the direction;
(ii) give a copy of the written record of the direction to the entity; and
(b) do so within 48 hours after the direction is given.

35AM Compliance with an information gathering direction

An entity must comply with a direction given to the entity under section 35AK to the extent that the entity is capable of doing so.

Civil penalty: 150 penalty units.

35AN Self-incrimination etc.

(1) An entity is not excused from giving information under section 35AK on the ground that the information might tend to incriminate the entity.

(2) If, at general law, an individual would otherwise be able to claim the privilege against self-exposure to a penalty (other than a penalty for an offence) in relation to giving information under section 35AK, the individual is not excused from giving information under that section on that ground.

Note: A body corporate is not entitled to claim the privilege against self-exposure to a penalty.

35AP Admissibility of information etc.

If information is given under section 35AK:
(a) the information; or
(b) giving the information;
is not admissible in evidence against an entity:
(c) in criminal proceedings other than proceedings for an offence against section 137.1 or 137.2 of the *Criminal Code* that relates to this Act; or
(d) in civil proceedings other than proceedings for recovery of a penalty in relation to a contravention of section 35AM.

Division 4—Action directions

35AQ Action direction

(1) If an entity is a relevant entity for:
(a) a critical infrastructure asset; or
(b) a critical infrastructure sector asset;
the Secretary may give the entity a direction that directs the entity to do, or refrain from doing, a specified act or thing within the period specified in the direction.

(2) The Secretary must not give a direction under this section unless the direction:
(a) is identical to a direction specified in a Ministerial authorisation; and
(b) includes a statement to the effect that the direction is authorised by the Ministerial authorisation; and
(c) specifies the date on which the Ministerial authorisation was given.

Note: A Ministerial authorisation must not be given unless the Minister is satisfied that the direction is reasonably necessary for the purposes of responding to a cyber security incident—see section 35AB.

(3) The period specified in the direction must end at or before the end of the period for which the Ministerial authorisation is in force.

(4) A direction under this section is subject to such conditions (if any) as are specified in the direction.

(5) The Secretary must not give a direction under this section that would require an entity to give information to the Secretary.

Other powers not limited

(6) This section does not, by implication, limit a power conferred by another provision of this Act.

35AR Form of direction

(1) A direction under section 35AQ may be given:
  (a) orally; or
  (b) in writing.

(2) The Secretary must not give a direction under section 35AQ orally unless the delay that would occur if the direction were to be given in writing would frustrate the effectiveness of the direction.

(3) If a direction under section 35AQ is given orally to an entity, the Secretary must:
  (a) do both of the following:
    (i) make a written record of the direction;
    (ii) give a copy of the written record of the direction to the entity; and
  (b) do so within 48 hours after the direction is given.

35AS Revocation of direction

Scope

(1) This section applies if:
  (a) a direction is in force under section 35AQ in relation to a Ministerial authorisation; and
  (b) the direction was given to a particular entity.

Power to revoke direction

(2) The Secretary may, by written notice given to the entity, revoke the direction.

Duty to revoke direction

(3) If the Secretary is satisfied that the direction is no longer required to respond to the cyber security incident to which the Ministerial authorisation relates, the Secretary must, by written notice given to the entity, revoke the direction.

Automatic revocation of direction

(4) If the Ministerial authorisation ceases to be in force, the direction is revoked.

Application of Acts Interpretation Act 1901

(5) This section does not, by implication, affect the application of subsection 33(3) of the *Acts Interpretation Act 1901* to an instrument made under a provision of this Act (other than this Part).

35AT Compliance with direction

(1) An entity commits an offence if:
  (a) the entity is given a direction under section 35AQ; and
  (b) the entity engages in conduct; and
  (c) the entity's conduct breaches the direction.

Penalty: Imprisonment for 2 years or 120 penalty units, or both.

(2) Subsection (1) does not apply if the entity took all reasonable steps to comply with the direction.

35AV Directions prevail over inconsistent obligations

If an obligation under this Act is applicable to an entity, the obligation has no effect to the extent to which it is inconsistent with a direction given to the entity under section 35AQ.

35AW Liability

(1) An entity is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith in compliance with a direction given under section 35AQ.

(2) An officer, employee or agent of an entity is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith in connection with an act done or omitted by the entity as mentioned in subsection (1).

Division 5—Intervention requests

35AX Intervention request

(1) The Secretary may give the chief executive of the authorised agency a request that the authorised agency do one or more specified acts or things within the period specified in the request.

(2) The Secretary must not give a request under this section unless the request:
  (a) is identical to a request specified in a Ministerial authorisation; and
  (b) includes a statement to the effect that the request is authorised by the Ministerial authorisation; and
  (c) specifies the date on which the Ministerial authorisation was given.

Note: A Ministerial authorisation must not be given unless the Minister is satisfied that the request is reasonably necessary for the purposes of responding to a cyber security incident—see section 35AB.

(3) The period specified in the request must end at or before the end of the period for which the Ministerial authorisation is in force.

(4) A request under this section is subject to such conditions (if any) as are specified in the request.

(5) A request under this section does not extend to:
  (a) doing an act or thing that would be prohibited by section 7 of the *Telecommunications (Interception and Access) Act 1979*; or
  (b) doing an act or thing that would be prohibited by section 108 of the *Telecommunications (Interception and Access) Act 1979*; or
  (c) doing an act or thing that would (disregarding this Act) be prohibited by section 276, 277 or 278 of the *Telecommunications Act 1997*.

Other powers not limited

(6) This section does not, by implication, limit a power conferred by another provision of this Act.

35AY Form and notification of request

(1) A request under section 35AX may be given:
  (a) orally; or
  (b) in writing.

(2) The Secretary must not give a request under section 35AX orally unless the delay that would occur if the request were to be given in writing would frustrate the effectiveness of the request.

Notification of requests given orally

(3) If a request under section 35AX is given orally, the Secretary must:
  (a) do both of the following:
    (i) make a written record of the request;
    (ii) give a copy of the written record of the request to the chief executive of the authorised agency; and
  (b) do so within 48 hours after the request is given.

(4) If a request under section 35AX is given orally in relation to a critical infrastructure asset, the Secretary must:
  (a) do both of the following:
    (i) make a written record of the request;
    (ii) give a copy of the written record of the request to the responsible entity for the asset; and
  (b) do so within 48 hours after the request is given.

(5) If a request under section 35AX is given orally in relation to a critical infrastructure sector asset (other than a critical infrastructure asset), the Secretary must:
  (a) make a written record of the request; and
  (b) give a copy of the written record of the request to whichever of the following entities the Secretary considers to be most relevant in relation to the request:
    (i) the owner, or each of the owners, of the asset;
    (ii) the operator, or each of the operators, of the asset; and
  (c) do so within 48 hours after the request is given.

Notification of requests given in writing

(6) If a request under section 35AX is given in writing, the Secretary must:
  (a) give a copy of the request to the chief executive of the authorised agency; and
  (b) do so within 48 hours after the request is made.

(7) If a request under section 35AX is given in writing in relation to a critical infrastructure asset, the Secretary must:
  (a) give a copy of the request to the responsible entity for the asset; and
  (b) do so within 48 hours after the request is given.

(8) If a request under section 35AX is given in writing in relation to a critical infrastructure sector asset (other than a critical infrastructure asset), the Secretary must:

(a) give a copy of the request to whichever of the following entities the Secretary considers to be most relevant in relation to the request:
  (i) the owner, or each of the owners, of the asset;
  (ii) the operator, or each of the operators, of the asset; and
(b) do so within 48 hours after the request is given.

35AZ Compliance with request

(1) The authorised agency is authorised to do an act or thing in compliance with a request under section 35AX.

(2) An act or thing done by the authorised agency in compliance with a request under section 35AX is taken to be done in the performance of the function conferred on the authorised agency by paragraph 7(1)(f) of the *Intelligence Services Act 2001*.

35BA Revocation of request

Scope

(1) This section applies if a request is in force under section 35AX in relation to a Ministerial authorisation.

Power to revoke request

(2) The Secretary may, by written notice given to the chief executive of the authorised agency, revoke the request.

Duty to revoke request

(3) If the Secretary is satisfied that the request is no longer required to respond to the cyber security incident to which the Ministerial authorisation relates, the Secretary must, by written notice given to the chief executive of the authorised agency, revoke the request.

Automatic revocation of request

(4) If the Ministerial authorisation ceases to be in force, the request is revoked.

Notification of revocation of request

(5) If a request under section 35AX is revoked, the Secretary must:
(a) give a copy of the revocation of the request to the chief executive of the authorised agency and each relevant entity for the asset; and
(b) do so as soon as practicable after the revocation.

Application of Acts Interpretation Act 1901

(6) This section does not, by implication, affect the application of subsection 33(3) of the *Acts Interpretation Act 1901* to an instrument made under a provision of this Act (other than this Part).

35BB Relevant entity to assist the authorised agency

(1) If:
(a) a request is in force under section 35AX in relation to a critical infrastructure asset or a critical infrastructure sector asset; and
(b) an entity is a relevant entity for the asset;

an approved staff member of the authorised agency may require the entity to:

(c) provide the approved staff member with access to premises for the purposes of the authorised agency complying with the request; or

(d) provide the authorised agency with specified information or assistance that is reasonably necessary to allow the authorised agency to comply with the request.

Note: See also section 149.1 of the *Criminal Code* (which deals with obstructing and hindering Commonwealth public officials).

(2) Paragraph (1)(c) does not apply to premises that are used solely or primarily as a residence.

(3) An entity must comply with a requirement under subsection (1).

Civil penalty: 150 penalty units.

Liability

(4) An entity is not liable to an action or other proceeding for damages for, or in relation to, an act done or omitted in good faith in compliance with a requirement under subsection (1).

(5) An officer, employee or agent of an entity is not liable to an action or other proceeding for damages for, or in relation to, an act done or omitted in good faith in connection with an act done or omitted by the entity as mentioned in subsection (4).

35BC Constable may assist the authorised agency

(1) If an entity refuses or fails to provide an approved staff member of the authorised agency with access to premises when required to do so under subsection 35BB(1):

(a) the approved staff member may enter the premises for the purposes of the authorised agency complying with the request mentioned in that subsection; and

(b) a constable may:

(i) assist the approved staff member in gaining access to the premises by using reasonable force against property; and

(ii) if necessary for the purposes of so assisting the approved staff member—enter the premises.

(2) If an approved staff member of the authorised agency has entered premises for the purposes of the authorised agency complying with a request under section 35AX, a constable may:

(a) assist the authorised agency in complying with the request by using reasonable force against property located on the premises; and

(b) for the purposes of so assisting the authorised agency—enter the premises.

35BD Removal and return of computers etc.

Removal of computers etc.

(1) If:

(a) in compliance with a request under section 35AX, the authorised agency adds or connects a computer or device to a computer network; and

(b) at a time when the request is in force, an approved staff member of the authorised agency forms a reasonable belief that the addition or connection of the computer or device is no longer required for the purposes of responding to the cyber security incident to which the relevant Ministerial authorisation relates;

the authorised agency must remove or disconnect the computer or device as soon as practicable after the approved staff member forms that belief.

(2) If:

(a) in compliance with a request under section 35AX, the authorised agency adds or connects a computer or device to a computer network; and

(b) the request ceases to be in force;

the authorised agency must remove or disconnect the computer or device as soon as practicable after the request ceases to be in force.

Return of computers etc.

(3) If:

(a) in compliance with a request under section 35AX, the authorised agency removes a computer or device; and

(b) at a time when the request is in force, an approved staff member of the authorised agency forms a reasonable belief that the removal of the computer or device is no longer required for the purposes of responding to the cyber security incident to which the relevant Ministerial authorisation relates;

the authorised agency must return the computer or device as soon as practicable after the approved staff member forms that belief.

(4) If:

(a) in compliance with a request under section 35AX, the authorised agency removes a computer or device; and

(b) the request ceases to be in force;

the authorised agency must return the computer or device as soon as practicable after the request ceases to be in force.

35BE Use of force against an individual not authorised

This Division does not authorise the use of force against an individual.

35BF Liability

Each of the following:

(a) the chief executive of the authorised agency;

(b) an approved staff member of the authorised agency;

(c) a constable;

is not liable to an action or other proceeding (whether civil or criminal) for, or in relation to, an act or matter done or omitted to be done in the exercise of any power or authority conferred by this Division.

35BG Evidentiary certificates

(1) The Inspector-General of Intelligence and Security may issue a written certificate setting out any facts relevant to the question of whether anything done, or omitted to be done, by the authorised agency, or an approved staff member of the authorised agency, was done, or omitted to be done, in the exercise of any power or authority conferred by this Division.

(2) A certificate issued under subsection (1) is admissible in evidence in any proceedings as prima facie evidence of the matters stated in the certificate.

35BH Chief executive of the authorised agency to report to the Defence Minister and the Minister

(1) If:

(a) the Secretary gives a request under section 35AX that was authorised by a Ministerial authorisation; and

(b) the authorised agency does one or more acts or things in compliance with the request;

the chief executive of the authorised agency must:

(c) prepare a written report that:

(i) sets out details of those acts or things; and

(ii) explains the extent to which doing those acts or things has amounted to an effective response to the cyber security incident to which the Ministerial authorisation relates; and

(d) give a copy of the report to the Defence Minister; and

(e) give a copy of the report to the Minister.

(2) The chief executive of the authorised agency must comply with subsection (1) as soon as practicable after the end of the period specified in the request and, in any event, within 3 months after the end of the period specified in the request.

35BJ Approved staff members of the authorised agency

(1) The chief executive of the authorised agency may, in writing, declare that a specified staff member of the authorised agency is an ***approved staff member of the authorised agency*** for the purposes of this Act.

(2) A declaration under subsection (1) is not a legislative instrument.

Division 6—Reports to the Parliamentary Joint Committee on Intelligence and Security

35BK Reports to the Parliamentary Joint Committee on Intelligence and Security

(1) If the Secretary gives one or more directions under section 35AK or 35AQ, or one or more requests under section 35AX, in relation to a cyber security incident, the Secretary must give the Parliamentary Joint Committee on Intelligence and Security a written report about the incident.

(2) The report must include a description of each of the directions or requests.

Explanatory Memorandum

Government Assistance

This Bill introduces a Government Assistance regime to respond to serious cyber security incidents that applies to all critical infrastructure sector assets. Government recognises that industry should and in most cases, will respond to the vast majority of cyber security incidents, with the support of Government where necessary. However, Government maintains ultimate responsibility for protecting Australia's national interests. As a last resort, the Bill provides for Government assistance to protect assets immediately prior, during or following a significant cyber attack.

Schedule 1—Security of critical infrastructure

Part 1—General amendments

Administrative Decisions (Judicial Review) Act 1977

Item 1 Before paragraph (da) of Schedule 1

1. Item 1 of Schedule 1 to the Bill inserts new paragraph (dae) into Schedule 1 to the ADJR Act, to provide that any decision made under new Part 3A of the SOCI is not a 'decision to which this Act applies'. This means that a decision made under new Part 3A in response to a 'serious cyber security incident' is not subject to judicial review under the ADJR Act (see further explanation regarding new Part 3A below).

2. The Administrative Review Council (ARC), in their 2012 report *Federal Judicial Review in Australia*, identified a number of reasons that may justify an exemption from review under the ADJR Act. National security considerations were one such reason identified by the ARC as justifying excluding ADJR Act review, particularly where sensitive information is involved which may be publicly disseminated through judicial proceedings.

3. When making a decision under new Part 3A of the SOCI Act, the Minister must be satisfied that there is a material risk that a 'cyber security incident' (as defined by new section 12M, see item 7 of Schedule 1 below) has seriously prejudiced, is seriously prejudicing, or is likely to seriously prejudice, the social or economic stability of Australia or its people, the defence of Australia or national security. Decisions of this nature are likely to be based on sensitive and classified information and deal with the capabilities of intelligence agencies as well as security vulnerabilities. This could include intelligence information and covert investigation methods and procedures, the disclosure of which may impact ongoing investigations, compromise intelligence methodologies or other damage Australia's national security and defence. The same applies equally to decisions of the Secretary and the authorised agency under new Part 3A who operationalise the Ministerial authorisations.

4. For this reason, it is reasonable to exempt decisions made under new Part 3A of the SOCI Act from review under the ADJR Act as the public dissemination of the sensitive information and capabilities that may be used to make decisions under new Part 3A would pose a risk to national security and the defence of Australia.

5. Similar to decisions made under the *Foreign Acquisitions and Takeovers Act 1975*, which are exempt from review under the ADJR Act (see paragraph (h) of Schedule 1 to that Act), decisions made under Part 3A are also likely to deal with classified and commercially confidential material that is relevant to the operation of assets critical to Australia's economy. This further supports the need for the exemption noting the potential impact to the economy if the confidentiality of this information was compromised.

6. Owners and operators of critical infrastructure assets may be reluctant or unwilling to disclose such information to government for the purpose of Part 3A, despite the penalties that such non-compliance could attract, if there is potential for this information to be disclosed publicly in court proceedings under the ADJR Act. This could delay or seriously inhibit the Minister, Secretary or authorised agency from making decisions under new Part 3A to protect assets critical to the Australian economy from imminent or released threats.

7. Furthermore, Part 3A is designed to be used in emergency circumstances where it is necessary for the Government to respond rapidly to the most serious cyber security incidents that are affecting critical infrastructure assets. Any unnecessary delays in the use of these mechanisms may prejudice the national interest noting the complex nature of such serious cyber security incidents, and the importance of critical infrastructure assets to Australia's social and economic stability, defence and national security. An exemption from review under the ADJR Act ensures the mechanisms in new Part 3A can be deployed as required and without delay.

8. Whilst decisions under new Part 3A will be exempt from review under the ADJR Act, there are certain safeguards and limitations included in the Bill to ensure that any decisions made under the Part are appropriate. In particular, the Minister can only make an authorisation for the exercise of powers where the Minister is satisfied that:

- a cyber security incident has occurred, is occurring or is imminent (paragraph 35AB(1)(a))
- the incident has had, is having, or is likely to have, a 'relevant impact' (as defined in new section 8G) on a critical infrastructure asset (paragraph 35AB(1)(b))
- there is a material risk that the incident has seriously prejudiced, is serious prejudicing, or is likely to seriously prejudice the social or economic stability of Australia or its people, defence or national security (paragraph 35AB(1)(c)), and
- no other regulatory system could be used to provide a practical and effective response to the incident (paragraph 35AB(1)(d)).

9. Further, consultation requirements are built into each stage of the regime to ensure any concerns of the entity are considered, and that any decisions are informed.

10. Importantly, the Inspector-General of Intelligence and Security will oversee the activities of the authorised agency under the Part. The Commonwealth Ombudsman also maintains jurisdiction in relation to any of the Secretary's activities under new Part 3A.

11. It is noted that the amendment does not have the effect of entirely excluding judicial review of decisions under Part 3A of the SOCI Act. A person who is the subject of a decision under Part 3A is still

entitled to seek judicial review under section 39B of the *Judiciary Act 1903* or subsection 75(v) of the Constitution.

Item 44 At the end of Part 3

12. Item 44 of Schedule 1 to the Bill inserts new section 35AAB into Part 3 of the SOCI Act.

Section 35AAB Liability

13. New section 35AAB of the SOCI Act limits the liability of an entity and its officers, employees or agents in relation to acts or omissions done in compliance of a direction made by the Minister under subsection 32(2).

14. Subsection (1) provides that an entity, being a responsible entity for a critical infrastructure asset that has been given a Ministerial direction under subsection 32(2), is not liable to an action or other proceeding for damages for or in relation to an act or omission done or omitted in good faith in compliance with a direction under subsection 32(2).

15. Subsection (2) provides that an officer, employee or agent of an entity is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith in connection with an act done or omitted by the entity as mentioned in subsection (1).

16. A direction made under section 32 may require an entity, or its officers, employees or agents, to do or stop doing certain things in order to address a security risk. Compliance with this power may result in the entity being liable. For example, a direction requiring an entity to cease using the services of a certain provider may result in them breaching contractual obligations with that provider. This provision will ensure that the entity, or its staff, will not be liable when acting in compliance with a lawful direction from the Minister.

Item 45 After Part 3

17. Item 45 of Schedule 1 to the Bill inserts new Part 3A (responding to critical cyber security incidents) into the SOCI Act. The government assistance powers conferred by Part 3A, exercisable under a Ministerial authorisation granted under Division 2, include powers to:

- gather information from an entity that may assist with determining whether a power under the SOCI Act should be exercised (Division 3)
- direct that an entity do, or refrain from doing, a specified act or thing (Division 4), and
- request that an authorised agency (i.e. ASD) intervene with an entity's operations (Division 5).

18. Existing Part 2 and new Part 2B of the SOCI Act, discussed above, impose obligations on industry to manage risks associated with the operation of critical infrastructure assets. As critical infrastructure assets are increasingly reliant on, and connected via, electronic systems, cyber security vulnerabilities are a matter of increasing and fundamental concern. As malicious actors are exploiting these vulnerabilities on an ever more frequent basis, including in relation to critical infrastructure assets, enhanced powers must be available.

Where serious risks do eventuate which affect the ability of the asset to deliver essential services and prejudice Australia's national interests, effective mechanisms are required to resolve the incident.

Globally, we have recently witnessed a number of cyber security incidents in relation to critical infrastructure assets that have had significant direct and indirect consequences. The impacts of these cyber incidents have ranged from large scale financial losses to loss of life.

Ukraine power outages, 2015

The 23 December 2015 Ukrainian power outages highlighted the impacts of cyber attacks on critical infrastructure. The attack involved sophisticated malicious actors taking command and control of the Supervisory Control and Data Acquisition (SCADA) systems of three energy distributors, resulting in 30 substations being switched off. The attack disabled or destroyed other digital infrastructure and wiped data from the companies' networks. An employee reportedly watched on helplessly as the malicious actor took substations offline. Concurrently, a call centre that provided up to date information to consumers about the blackout became inoperable due to a denial-of-service attack. While less than 1 per cent of the country's daily consumption of energy was disrupted, the attack left over 225,000 Ukrainians, in the middle of winter, without power for several hours. Two months after the attack, some control centres were still not fully operational with manual procedures required. However, the potential for far greater consequences remain. Cyber attacks can destroy physical components. With the capability and intent, an attack on the energy sector could result in impacts that are significantly more difficult to repair.

WannaCry, 2017

In 2017, a large-scale ransomware campaign, commonly called WannaCry, affected some 230,000 individuals and over 300,000 computer systems in 150 countries. The incident resulted in an estimated USD$4 billion in financial losses globally. WannaCry targeted vulnerabilities in Microsoft Windows software, impacting communications, financial, transport and healthcare services. This included the United Kingdom's National Health Service which was forced to turn away non-critical patients and cancel around 20,000 appointments.

Hospital attacks, 2020

Since the COVID-19 pandemic began, hospitals have come under increasing strain due to malicious cyber incidents, particularly ransomware attacks. The March 2020 ransomware attack on Brno University Hospital, one of the Czechia's largest COVID-19 testing laboratories, saw the forced shut down of its entire information technology network. In September 2020, Dusseldorf University Hospital suffered a ransomware attack that brought

down its computer systems. As a result, an individual being transported to the hospital by ambulance was re-routed to another hospital 30 kilometres and passed away en route.

19. The Government remains committed, first and foremost, to working in partnership with states, territories and industry, who own, operate and regulate our critical infrastructure to collaboratively resolve incidents when they do occur and mitigate their impacts. Collaborative resolution will always remain the most effective method of resolving and incident and the Government's first preference. However, noting the importance of the services being provided by these assets and the Government's ultimate responsibility for protecting Australia's national interests, circumstances may arise which require Government intervention. In such emergency circumstances, it is crucial that the Government has last resort powers to respond to the incident or mitigate the risk.

20. Part 3 of the SOCI Act currently provides the Minister for Home Affairs with the power to issue a direction to a reporting entity or operator to require them to take action to mitigate risks that are prejudicial to security. However, as critical infrastructure assets have become increasingly reliant on cyber infrastructure, and noting the rapidly evolving cyber threat environment we currently face, an additional emergency regime is required to address the risk of a particularly serious cyber attack which seriously prejudices Australia's national interests. Without such powers, a single cyber attack could have cascading catastrophic, life threatening consequences.

21. Consultations have revealed a strong community expectation that, in emergency circumstances and as a matter of last result, the Government will use its significant technical expertise in cyber-defence to protect Australia's national interests and restore the functioning of essential services. However, consultations also highlighted that these powers must be used only in the most exceptional circumstances. The framework in Part 3A, as discussed below, is subject to a range of stringent safeguards and limitations to ensure that it is only used in the most serious circumstances, in an appropriate manner, and firmly limited to responding to the cyber security incident.

Division 1—Simplified outline of this Part

Section 35AA Simplified outline of this Part

22. New section 35AA of the SOCI Act sets out a simplified outline of Part 3A. The part provides the Government with certain limited powers to respond to serious cyber security incidents that are impacting critical infrastructure assets.

Division 2—Ministerial authorisation relating to cyber security incident

Section 35AB Ministerial authorisation

23. New section 35AB of the SOCI Act sets out the circumstances in which the Minister may give an authorisation for the Secretary to exercise the government assistance powers under Part 3A in relation to a 'cyber security incident'. 'Cyber security incident' is newly defined in section 12M of the SOCI Act (see Item 32 of Schedule 1 to the Bill above) and includes acts, events or circumstances involving:

- unauthorised access to computer data or a computer program (paragraph (a))
- unauthorised modification of computer data or a computer program (paragraph (b)),
- unauthorised impairment of electronic communications to or from a computer (paragraph (c)), and
- unauthorised impairment of the availability, reliability, security or operation of a computer, computer data or a computer program (paragraph (d)).

Subsection 35AB(1)—Scope

24. Subsection 35AB(1) creates a high threshold for when a ministerial authorisation can be made under subsection 35AB(2), and ensures that the powers in Part 3A are only used in emergency circumstances, as a last resort and when it is in the national interest. In practice, subsection 35AB(1) ensures that the Secretary will only be authorised by the Minister to use the powers in Part 3A in exceptionally rare or emergency circumstances.

25. Subsection (1) provides that section 35AB applies where the Minister is satisfied of all of the following matters:

- a cyber security incident has occurred, is occurring or is imminent (paragraph (a))
- the incident has had, is having or is likely to have a relevant impact on a critical infrastructure asset, known as the 'primary asset' (paragraph (b))
- there is a material risk that the incident has seriously prejudiced, is seriously prejudicing or is likely to seriously prejudice the social or economic stability of Australia or its people, the defence of Australia or national security (including security and international relations) (paragraph (c)), and
- no existing regulatory system of the Commonwealth, a State or a Territory could be used to provide a practical and effective response to the incident (paragraph (d)).

26. Each of these factors is discussed in turn below.

Paragraph 35AB(1)(a)—A cyber security incident has occurred, is occurring or is imminent

27. Firstly, the Minister must be satisfied that a cyber security incident has occurred, is occurring, or is imminent. Cyber security incident is defined at new section 12M and, broadly speaking, means one or more acts, events or circumstances involving unauthorised access, modification or impairment of computer data, a computer program or a computer.

28. This limits the focus of Part 3A to responding to cyber security incidents. As critical infrastructure assets are increasingly reliant on, and connected via, electronic systems, cyber security vulnerabilities are a matter of increasing and fundamental concern. The Government has particular expertise in responding to cyber threats that may not be available in the private sector.

29. Paragraph (1)(a) also relates to cyber security incidents that have occurred, are occurring or are imminent. A cyber security incident may come with warning, or suddenly, and be rapid or prolonged, but nevertheless catastrophic in its impact. This temporal scope is necessary to ensure that the Government may, where all the other criteria are met, provide an effective response as the circumstances require (examples below).

- There may be a credible threat, evidenced by positioning and potentially attacks on related infrastructure, that a malicious actor is about to launch a cyber attack. Therefore it is vital that the Government, when aware an attack is imminent, can if necessary take action to bolster defences in relation to the critical infrastructure asset in order to attempt to prevent the incident, and its consequential impact, from eventuating.

- An attack may occur unexpectedly and action is required to mitigate the impact, including by limiting the extent of compromise. This may include taking steps to prevent further compromise within a network or segregate systems to limit further damage.

- Where a cyber security incident has occurred, its impact may be significant and sustained. Even after the compromise has been addressed, significant work may be required to restore the functioning of the asset to enable it to recommence providing essential services.

Paragraph 35AB(1)(b)—The cyber security incident has had, is having, or is likely to have, a relevant impact on a critical infrastructure asset

30. Secondly, the Minister must be satisfied that the cyber security incident has had, is having, or is likely to have, a relevant impact on a critical infrastructure asset. The exclusive objective of this regime is to defend critical infrastructure assets, in light of their criticality to the social or economic stability of Australia or its people, the defence of Australia, or national security. That is to say, this is not intended to be a regime that can be used to defend assets economy-wide. While cyber security incidents can have significantly and costly impacts on assets which are not critical, the ability for the Government to step-in is exclusively reserved for critical infrastructure assets given the essential services they provide to the nation. Nevertheless, the Government is committed to working collaboratively with those other entities through other non-regulatory mechanisms to improve cyber resilience and response capabilities.

31. Section 8G provides the definition of a relevant impact in this context, which includes an impact on the availability, integrity, reliability or confidentiality of the asset. The use of relevant impact in paragraph (1)(b) means that a ministerial authorisation cannot be made if the impact, or the likely impact, of the cyber security incident is not sufficiently serious. For example, impacting the profitability of an asset. Rather, the regime is more focused on impact that undermine the intended operation or functioning of a critical infrastructure asset, or put at risk the asset's networks and sensitive information holdings.

32. A relevant impact may occur directly or indirectly. That is to say that a cyber security incident can have a relevant impact on a critical infrastructure asset, even if for example, the incident does not involve a direct compromise of the critical infrastructure asset's systems. This reflects that, due to the complex and extensive interdependencies of critical infrastructure assets, a cyber security incident can significantly impede or compromise the functioning of an asset by targeting a crucial dependency in its supply chain

rendering the primary asset inoperable. Therefore, Ministerial authorisation may be made in relation to critical infrastructure sector assets, meaning assets that relate to a critical infrastructure sector.

Paragraph 35AB(1)(c)—Material risk that the incident has seriously prejudiced, is seriously prejudicing, or is likely to serious prejudice

33. Thirdly, the Minister must be satisfied that there is a material risk that the incident has seriously prejudiced, is seriously prejudicing, or is likely to seriously prejudice:

- the social or economic stability of Australia or its people; or
- the defence of Australia; or
- national security.

34. This criteria is important in establishing that the event must be of significant seriousness. That is, Australia's national interests are at risk. The executive arm of government is best placed to make this assessment, as it requires consideration of a wide range of varying factors on a case by case basis. In particular, this assessment is likely to rely on intelligence about the potential cascading impact of the incident.

35. 'Seriously prejudiced' has its ordinary meaning. In the context of new paragraph 35A(1)(c), the use of 'seriously prejudiced' is designed to ensure that a ministerial authorisation is not made unless the Minister is satisfied that the impact, or likely impact, of the cyber security incident on a critical infrastructure asset can reasonably be considered capable of causing significant damage or harm to Australian interests. To clarify, the Minister may be satisfied that an incident meets this criterion even if it is not impacting on all jurisdictions. Instead, the focus of this provision is on the impact to Australia's various national interests, recognising that an impact on, for example, a particular part of the economy may be nationally significant.

Paragraph 35AB(1)(d)—There is no existing regulatory system that could be used to provide a practical and effective response to the incident

36. Finally, the Minister must be satisfied that there is no existing regulatory system of the Commonwealth, a State or a Territory that could be used to provide a practical and effective response to the incident. This requirement is intended to cement this power as one of last resort, acknowledging the various regulatory regimes that exist across governments which may be utilised to manage risks. However, where those risks exceed the capacity of those systems, this regime will offer an effective and practice response. This ensures that, wherever possible and appropriate, consideration is given to whether existing regimes, which are potentially less invasive or which are designed specifically to address risks associated with particular assets, could be relied upon to effectively respond to the incident.

37. The Minister can be satisfied of this even if those other systems, if any, have not attempted to be used so long as the Minister considers that if they used, they would not provide a practical and effective response. This is to ensure that futile steps are not required to be taken and shown to fail in time critical situations before an effective response can be initiated. In satisfying themselves of this requirement, the Minister is likely to consult with relevant Commonwealth, State and Territory Ministers, as well as regulators, including

any relevant Commonwealth regulator designated under the amended SOCI Act. This may also include receiving referrals for action when an event has escalated beyond their abilities.

Hypothetical scenario:

A large energy provider has been the subject of a cyber security incident which impacts its ability to provide electricity to residents of the east coast of Australia. As a result, large population hubs are without electricity and there are cascading impacts to other critical infrastructure assets such as outages to critical telecommunications assets and critical hospitals causing widespread economic and social disruption.

The Commonwealth has consulted with the relevant State regulator who has advised that they do not have the powers to effectively respond to the incident, and has requested the Commonwealth provide assistance.

Subsections 35AB(2)-(4)—Ministerial authorisation

38. When satisfied of the factors in subsection (1), subsection (2) provides that the Minister may, on application by the Secretary, do any or all of the following things:

- authorise the Secretary to give directions to a specified entity under section 35AK (information gathering directions) that relate to the incident and the 'primary asset' or a specified critical infrastructure sector asset (paragraphs (a) and (b))
- authorise the Secretary to give directions to a specified entity under section 35AQ (action directions) that relate to the incident and the primary asset or a specified critical infrastructure sector asset (paragraphs (c) and (d)), or
- authorise the Secretary to give a specified request under section 35AX (intervention request) that relates to the incident and the primary asset or a specified critical infrastructure sector asset (paragraphs (e) and (f)).

39. Subsection (3) provides that an authorisation made by the Minister under subsection (2) is to be known as a 'Ministerial authorisation'.

40. These various forms of Ministerial authorisation must relate to the cyber security incident, and be made in relation to the primary asset or a specified critical infrastructure sector asset. While in most circumstances, the primary asset will be the focus of the ministerial authorisation, in some circumstances, a Ministerial authorisation may be required in relation to a critical infrastructure sector asset.

41. This reflects that, due to the complex and extensive interdependencies of critical infrastructure assets, a cyber security incident can significantly impede or compromise the functioning of an asset by targeting a crucial dependency in its supply chain rendering the primary asset inoperable. As a result, it may be necessary for defensive action to be taken in relation to an asset other than the critical infrastructure asset itself, although the action must be focused on the protection and restitution of the critical infrastructure asset. This will ensure that the necessary intervention can be made at the most appropriate and effective place

within the ecosystem of the critical infrastructure asset. However, the Ministerial authorisation must be made in relation to a critical infrastructure sector asset, limiting the operation of the regime to the critical infrastructure sectors.

42. For example, the Minister may authorise the Secretary to give directions to a specified entity in relation to a specified critical infrastructure sector asset that provides information technology services to a critical infrastructure asset. This may be necessary to better understand the operation of the critical infrastructure asset and inform the Government's understanding of the nature and extent of a cyber compromise. Similarly, a critical infrastructure sector asset may be used as a vector or platform for an attack on a critical infrastructure asset due to connectivity between the respective assets' systems. Therefore an effective response to the incident may need to be made in relation to the critical infrastructure sector asset to assist in mitigating the impacts on the critical infrastructure sector asset.

43. Further, Ministerial authorisations under paragraphs (c)-(d) must specify the direction or request that is being authorised. The Secretary, when taking steps in response to the authorisation, does not have discretion to expand the scope of actions that can be directed or requested. The significance of Ministerial authorisations made under those paragraphs make it appropriate for their scope to be determined by the Minister.

44. Subsection (4) provides that subsection 33(3AB) of the Acts Interpretation Act, that relevantly provides that a Ministerial authorisation under subsection (2) could be made with respect to a class of assets or cyber security incidents, does not apply. This is appropriate and necessary to include given the serious and invasive nature of the government assistance powers that can be exercised as a result of a Ministerial authorisation, with the effect being that the Minister will need to consider the unique circumstances of each entity to which the authorisation will apply.

Subsections 35AB(5)-(6)—Information gathering directions

45. The first type of Ministerial authorisation that can be made relate to the gathering of information. An effective and appropriate response to a serious cyber security incident requires a strong understanding of the nature and extent of the incident, as well as a strong understanding of the circumstances of the asset including its cyber maturity, its vulnerabilities and its interdependencies. This information will inform any decisions in relation to further Ministerial authorisations, and be important in ensuring that those Ministerial authorisations are reasonably necessary and proportionate.

46. Subsection (5) provides that a Ministerial authorisation under paragraph (2)(a) or (b), enabling the Secretary to give directions under section 35AK, is generally applicable to the incident and the asset concerned, and is to be made without reference to any specific directions.

47. Under subsection (6), the Minister must not give a Ministerial authorisation under paragraph (2)(a) or (b) unless the Minister is satisfied that the directions under section 35AK that could be authorised by the Ministerial authorisation are likely to facilitate a practical and effective response to the incident.

48. These subsections provide that the Minister may authorise the Secretary utilising information gathering directions (when the factors outlined in section 35AK are met) if doing so is likely to facilitate a practical and effective response to the incident. For example, the Minister may consider that the use of the

powers in section 35AK are necessary to facilitate a practical and effective response to the incident, where the Minister is aware of the severity of the incident but is unsure as to what actions are needed to respond.

49. In comparison to Ministerial authorisations made under paragraphs (2)(c)-(f), the authorisation will not specify the precise content of the direction or directions that can be made by the Secretary. Noting that this provides the Secretary with a degree of discretion in developing information gathering directions, that discretion is limited by section 35AK to ensure that the power is only used in an appropriate way. Further, it is noted that this information gathering power can be used in relation to critical infrastructure sector assets, while in comparison the Secretary's existing information gathering powers provided in existing section 37 of the SOCI Act are limited to being in relation to critical infrastructure assets. This broader scope is warranted as the interdependencies between critical infrastructure assets and other assets across the critical infrastructure sectors may mean that information necessary to guide an effective response is held by an entity related to another asset which relates to the critical infrastructure sector.

Hypothetical scenario:

A key supplier of logistical services to a critical freight service asset is subject to a cyber security incident which results in the critical freight service asset being unable to distribute medical supplies nationally. While the responsible entity for the critical freight service asset is cooperating with government, the Government requires information from the provider of the logistical services to determine the full extent of the compromise and develop an appropriate response.

The Minister for Home Affairs authorises the Secretary of Home Affairs issuing information gathering directions to the supplier, as the entity responsible for the critical infrastructure sector asset, to provide the necessary information. This information is used to jointly develop an appropriate response with the responsible entity to mitigating the impacts of the incident on the critical freight service asset.

Subsections 35AB(7)-(9)—Action directions

50. The second type of Ministerial authorisation that can be made relate to requiring the specified entity to do an act or thing, including an omission. In responding to an incident, the Government acknowledges that an entity's understanding of the systems and operation of the asset means that the entity is best positioned to take the necessary actions to respond to the incident. Therefore, this type of Ministerial authorisation is focused on compelling the entity to take actions, or do things, that are reasonably necessary and proportionate to responding to the incident where the entity is unwilling or unable to respond to the incident.

51. Subsection (7) provides that the Minister must not give a Ministerial authorisation under paragraphs (2)(c) or (d), enabling the Secretary to give action directions under section 35AQ, unless the Minister is satisfied of the existence of the circumstances set out in paragraphs (a) to (d). It should be noted that these criteria are additional to those criteria in subsection (1) of which the Minister must also be satisfied.

52. Firstly, the Minister must be satisfied that the entity is unwilling or unable to take all reasonable steps to respond to the incident (under paragraph (7)(a)). This is reflective of the Government's continued view that industry are primarily responsible for responding to cyber security incidents and that Government intervention is only to be used in emergencies and as a last resort when industry fail to resolve the incident. The unwillingness of an entity to take all reasonable steps may be driven by various factors, such as profit, reputation, or external influence. However noting the criticality of the asset and the impact of the incident, as well as the material risk of serious prejudice to Australia's national interest, in these circumstances resolving the incident must take precedence. The inability of an entity to take all reasonable steps may be driven by a technical lack of capacity or capability, or legal constraints such as contractual or legislative requirements relating to continuity of service. Therefore, despite a willingness to resolve the incident, the entity may not be able to do so. For example, an entity may be willing to provide assistance voluntarily however is concerned about incurring liability for disclosing commercially confidential information and in such circumstances may request a Ministerial authorisation be made to facilitate them taking the necessary steps to assist in resolving the incident.

53. When considering what reasonable steps to respond to the incident may involve, it is not intended that a different tactical response to that which the Minister would pursue would amount to an unwillingness or inability to take reasonable steps to respond to the incident. The inclusion of the element of reasonableness will require the Minister to consider the various approaches that may be taken to effectively respond to the incident, with steps likely to be considered reasonable if they are capable of effectively and practically resolving the incident. The focus is on ensuring that an adequate response is taken, rather than being prescriptive of the exact response that must be taken.

54. However, it is important to note that certain steps may be regarded as reasonable even if they exceed the capacity or capabilities of the particular entity. Therefore consideration of whether all reasonable steps are being taken will require consideration of what a reasonable person would expect a business in that position to do or be able to do.

55. Secondly, the Minister must be satisfied that the specified direction is reasonably necessary for the purposes of responding to the incident (under paragraph (7)(b)). This provision appropriately limits the scope of an action direction to ensure it is directly relevant to addressing or responding to the incident. The use of 'reasonably necessary' clarifies that an action direction and anything that compliance with it would require to be done must be directly focused on responding to the incident. This is an important safeguard to ensure an action direction cannot be used as a vehicle to require an entity to do, or refrain from doing, an act that goes beyond addressing or responding to the incident. This reflects that this regime is only to be used to defend critical infrastructure assets from cyber security incidents, and is strictly limited to that purpose. Further the element of reasonableness will ensure that the required actions are not only necessary but are appropriate in the circumstances.

56. Thirdly, the Minister must be satisfied that the specified direction is a proportionate response to the incident (under paragraph (7)(c)). This provision appropriately limits the scope of an action direction to ensure it is proportionate. While the criteria the Minister must be satisfied of, as set out in subsection (1), highlight that the circumstance in which these powers will be used must be serious, it is equally important that the directions are proportionate in light of all the circumstances. For example, and depending on the

particular circumstances, a direction may not be regarded as proportionate if it would result in greater harm to the asset even if it would practically respond to the incident.

57. In considering proportionality, subsection (8) requires the Minister to have regard to the impact of the direction on the activities carried on by the specified entity and the functioning of the asset concerned, the consequences of compliance with the direction and any other matters the Minister considers relevant. For example, while taking a computer system offline may be reasonably necessary to mitigating a cyber security incident, if that computer system is necessary for providing life sustaining equipment, the Minister will need to consider the respective consequences of action and inaction, and whether alternative options are available. Additionally, the Minister may consider the costs for the entity in complying and whether the costs from action would outweigh the costs of inaction, including for the entity and society more broadly. The impact on end-users and customers of the asset may also be relevant considerations in considering proportionately.

58. Finally, the Minister must be satisfied that the specified direction is technically feasible (under paragraph (7)(d)). A direction is technically feasible when the direction relates to a course of action that is reasonably possible to execute, or within the existing capability of the relevant entity. A direction is considered not to be technically feasible if there is no technical capability that could be utilised to produce the outcome that is sought. The consultation requirement in section 35AD will be an important mechanism to ensure the Minister has a sound understanding of the entities technical capabilities and therefore whether this condition is met.

59. Subsection (9) provides further limitations on the scope of what can be authorised by the Minister. A direction must not:

- require the specified entity to permit the authorised agency to do an act or thing that could be the subject of a request under section 35AX (paragraph (a)), or
- require the specified entity to take offensive cyber action against a person who is directly or indirectly responsible for the incident (paragraph (b)).

60. Noting that a Ministerial authorisation in relation to an intervention request is subject to additional safeguards due to the significance of the conduct that may be authorised, paragraph (a) ensures that action directions are not used as a backdoor to compel an entity to permit Government officials access to the asset. Further paragraph (b) embeds the defensive nature of the regime, noting that it would not be appropriate to require the entity to take actions against the perpetrator of the attack that are not regarded as defensive. For example, the directions cannot require the entity to 'hack back' or undertake any other actions that may constitute a criminal offence such as accessing the perpetrators computer without authority. The focus of these directions is on defending the asset, which may include removing a perpetrator from the asset, but should not extend into actions that would be regarded as offensive. Paragraph (b) does not limit in anyway the responsibilities and powers that other agencies such as the Australian Signals Directorate and Australian Federal Police have to prevent and disrupt cybercrime under other legislative regimes.

Hypothetical scenario:

A critical data storage or processing asset, which hosts sensitive Government information, is subject to a cyber security incident which poses an imminent risk that the confidentiality of the Government information will be compromised. In light of information provided in response to information gathering directions, the Minister for Home Affairs is satisfied that the reconfiguration of the computer network to segregate the compromised computer and prevent the exfiltration of the sensitive Government information is reasonably necessary and proportionate to responding to the incident. Following consultation with the operator of the asset, the Minister for Home Affairs is also satisfied that the entity is unwilling to undertake the required action as it would affect, albeit in a limited way, the provision of services to the data centre's other customers.

Subsections 35AB(10)-(15)—Intervention requests

61. The third type of Ministerial authorisations that can be made relate to intervention requests. Where directing an entity to take specified action would not be practical or effective, it may be necessary for the Government to step-in and take the necessary actions to defend the asset. This is a last resort option, within a last resort regime, and will only be used in extraordinary circumstances. However it must be recognised that in emergencies where **Australia's** national interests are at risk of serious prejudice and industry is unable to respond, the Government may have unique expertise that could be deployed to prevent an incident, mitigate its impact, or restore the functioning of an asset following an incident. In some circumstances, the cyber capabilities and technical resources of the Australian Signals Directorate will surpass those of industry. Where those circumstances exist, it is reasonable, appropriate and expected that the Government has the powers to respond. Nevertheless, the significance of these powers necessity that they are subject to stringent safeguards, limitations and oversight mechanisms to ensure they are only used when absolutely necessary and appropriate.

62. Subsection (10) provides that the Minister must not give a Ministerial authorisation under paragraphs (2)(e) or (f), enabling the Secretary to make a request under section 35AQ, unless the Minister is satisfied of the existence of the circumstances set out in paragraphs (a) to (g). It should be noted that these criteria are additional to those criteria in subsection (1) of which the Minister must also be satisfied.

63. Firstly, the Minister must be satisfied that giving a Ministerial authorisation under paragraph (2)(c) or (d) would not amount to a practical and effective response to the incident (under paragraph (10)(a)). Direct Government intervention in relation to assets is appropriately reserved for extraordinary circumstances. To guarantee that this option is only considered as a last resort, the Minister must be satisfied that legally compelling the entity to do the action would not amount to a practical and effective response to the incident. For example, where the Minister has authorised a direction providing that the entity is to take the action and they have unreasonably refused to comply with the direction, the Minister may be satisfied that the directions power is not effective. Alternatively, following consultation, the Minister may be aware that the required actions require a level of technical expertise that the entity does not possess, and is not able to acquire, and therefore a ministerial authorisation for a direction to take the action would not be practical.

64. The Minister is not required to have made an authorisation under paragraph (2)(c) or (d) before the Minister can be satisfied that it would not amount to a practical and effective response to the incident. Noting the time critical nature of responding to the serious cyber security incident, a requirement to make futile Ministerial authorisations would not be reasonable. Rather, the Minister may, for example, be satisfied of this matter having consider information provided through consultation and information gained through directions issued by the Secretary under section 35K.

65. Secondly, paragraphs (10)(b) and (c) require the Minister be satisfied that the relevant entity or entities are unwilling or unable to take all reasonable steps to respond to the incident. This provision reflects that there may be multiple relevant entities that have a degree of responsibility for a particular aspect of the asset and may be in a position to take the necessary action. The Minister must be satisfied that none of these entities are willing or able to do so.

66. A relevant entity for an asset is defined in section 5 as an entity that is the responsible entity for the asset, a direct interest holder in relation to the asset, an operator of the asset, or is a managed service provider for the asset.

67. This is reflective of the Government's continued view that industry are primarily responsible for responding to cyber security incidents and that Government intervention is only to be used in emergencies and as a last resort when industry fail to resolve the incident. The unwillingness of an entity to take all reasonable steps may be driven by various factors, such as profit, reputation, or external influence. However noting the criticality of the asset and the impact of the incident, as well as the material risk of serious prejudice to Australia's national interest, in these circumstances resolving the incident must take precedence. The inability of an entity to take all reasonable steps may be driven by a technical lack of capacity or capability, or legal constraints such as contractual or legislative requirements relating to continuity of service. Therefore, despite a willingness to resolve the incident, the entity may not be able to do so. For example, an entity may be actively attempting to resolve the incident however the advanced nature of the compromise exceeds their technical expertise.

68. When considering what reasonable steps to respond to the incident may involve, it is not intended that a different tactical response to that which the Minister would pursue would amount to an unwillingness or inability to take reasonable steps to respond to the incident. The inclusion of the element of reasonableness will require the Minister to consider the various approaches that may be taken to effectively respond to the incident, with steps likely to be considered reasonable if they are capable of effectively and practically resolving the incident. The focus is on ensuring that an adequate response is taken, rather than being prescriptive of the exact response that must be taken.

69. However, it is important to note that certain steps may be regarded as reasonable even if they exceed the capacity or capabilities of the particular entity. Therefore consideration of whether all reasonable steps are being taken will require consideration of what a reasonable person would expect a business in that position to do or be able to do.

70. Thirdly, paragraph (10)(d) requires that the Minister be satisfied that the specified request is reasonably necessary for the purposes of responding to the incident. This provision appropriately limits the scope of an action that can be requested to ensure it is directly relevant to addressing or responding to the

incident. The use of 'reasonably necessary' clarifies that a request and anything that compliance with it would require to be done must be directly focused on responding to the incident. This is an important safeguard to ensure a request, and any action taken in response to that request, cannot be used for any purposes other than responding to the incident. This reflects that this regime is only to be used to defend critical infrastructure assets from cyber security incidents, and is strictly limited to that purpose. Further the element of reasonableness will ensure that the required actions are not only necessary but are appropriate in the circumstances.

71. Fourthly, paragraph (10)(e) requires that the Minister be satisfied that the specified request is a proportionate response to the incident. This provision appropriately limits the scope of a request, and the actions that may be taken in response to it, to ensure it is proportionate. While the criteria the Minister must be satisfied of, as set out in subsection (1), highlight that the circumstance in which these powers will be used must be serious, it is equally important that the directions are proportionate in light of all the circumstances. For example, and depending on the particular circumstances, a request may not be regarded as proportionate if the actions that may be taken in response to it would result in greater harm to the asset even if it would practically respond to the incident.

72. In considering proportionality, subsection (11) requires the Minister to have regard to the impact of compliance with the request on the functioning of the asset concerned, the consequences of compliance with the specified request, and any other matters the Minister considers relevant. For example, while taking a computer system offline may be reasonably necessary to mitigating a cyber security incident, if that computer system is necessary for providing life sustaining equipment, the Minister will need to consider the respective consequences of action and inaction, and whether alternative options are available. Further, the consequences of the requested actions on the asset itself, its longer-term functioning and associated costs, may also be considered. The impact on end-users and customers of the asset may also be relevant considerations in considering proportionately. The Minister may also consider the appropriateness of direct Government intervention in relation to a privately owned asset and whether the significance of that step is proportionate in light of the incident and its impacts.

73. Fifthly, paragraph (10)(f) requires that the Minister be satisfied that compliance with the specified request is technically feasible. While the Australian Signals Directorate has extensive and sophisticated capabilities, its resources are not without bounds. Therefore the Minister must consider whether it would be technically feasible for ASD to undertake the required action. Consultation between the Minister and the Minister for Defence will be important in determining whether the required actions are technically feasible.

74. Finally, paragraph (10)(g) requires that the Minister be satisfied that each of the acts or things specified in the request are acts or things covered by section 35AC. This regime is focused exclusively on cyber security incidents, and founded on the understanding that in some circumstances, the cyber capabilities and resources of the Australian Signals Directorate will surpass those of industry. Reflective of this, the actions requested must be limited to the computer related actions for which the Australian Signals Directorate has expertise in and must not extend more broadly.

75. Subsection (12) provides further limitations on the scope of what can be authorised by the Minister. The Minister must not give a Ministerial authorisation under paragraphs (2)(e) or (f) if compliance with the

specified request would involve the authorised agency taking offensive cyber action against a person who is directly or indirectly responsible for the incident. This limitation embeds the defensive nature of the regime, noting that it would not be appropriate to require to require the entity to take actions against the perpetrator of the attack that are not regarded as defensive. For example, the request cannot require the authorised agency to 'hack back' or undertake any other actions against a perpetrator. The focus of this regime is on defending the asset, which may include removing a perpetrator from the asset, but should not extend into actions that would be regarded as offensive. This subsection does not limit in anyway the responsibilities and powers that the ASD may have to prevent and disrupt cybercrime under other legislative regimes.

76. Subsection (13) provides an additional layer of oversight to reflect the significance of these powers. The Minister must not give a Ministerial authorisation under paragraphs (2)(e) or (f) unless the Minister has obtained the agreement of the Prime Minister and the Defence Minister.

77. The Prime Minister, as leader of the country and chair of the National Security Committee of Cabinet, is well positioned to assess the appropriateness of such an authorisation. The Defence Minister, as the minister responsible for the authorised agency, will ensure that their involvement is appropriate and consistent with other defence priorities and interests. This ensures that an authorisation for an intervention request is subject to a comprehensive triple lock mechanism, and any action that is intended to be conducted by the authorised agency has been scrutinised by key members of the executive arm of Government. The involvement of the Prime Minister and the Defence Minister will also add additional perspective and balance to the decision making process to ensure the impact on the entity is appropriate in the circumstances.

78. The agreement required by this subsection may be given orally or in writing (subsection (14)) noting the potential urgency of an effective response. However subsection (15) provides that, if agreement is given orally by either the Prime Minister or Defence Minister for the purposes of subsection (13), the respective Minister must make a written record of the agreement and give a copy of the written record to the Minister within 48 hours after the agreement is given.

Hypothetical Scenario:
During incident response, the authorised agency may require access to various types of data and information, such as systems logs and host images, to determine what malicious activity had occurred and what systems have been affected. The authorised agency may also need to install investigation tools, such as host-based sensors or network monitoring capabilities, to analyse the extent of malicious activity and inform effective remediation actions.

To remediate the cyber security incident, the authorised agency may need to remove malicious software (e.g. web shells, ransomware, and/or reconnaissance tools) which requires altering/removing of data in a computer. The authorised agency may need to conduct these activities on-site with the victim or remotely, where capability exists to do so.
The authorised agency may also implement blocking of malicious domains, may disable internet access or may implement other specified mitigations. The authorised agency may also require systems to be patched (altering data) or a change in network configurations, to alter the function of the system, to prevent a similar activity.

A Ministerial authorisation may be sought for an intervention request relating to each of these specific actions.

Subsection 35AB(16)—Ministerial authorisation is not a legislative instrument

79. Subsection (16) clarifies that a Ministerial authorisation given by the Minister under subsection (2) is not a legislative instrument. This is reasonable in these circumstances because:

- the public disclosure of an authorisation for intervention request may not only undermine the ability for the authorised officer to undertake any acts that have been authorised, but may also alert nefarious actors to a potential weakness or vulnerability in a critical infrastructure asset, and

- the authorisation applies the law in a particular circumstance to particular facts, and does not determine or alter the content of the law for the purposes of subsection 8(4) of the Legislation Act.

Subsection 35AB(17)—Other powers not limited

80. Subsection (17) provides that section 35AB does not, by implication, limit a power conferred by another provision of the SOCI Act.

Section 35AC Kinds of acts or things that may be specified in an intervention request

81. New section 35AC of the SOCI Act outlines the kinds of acts or things that a Ministerial authorisation under paragraphs 35AB(2)(e) or (f) may specify in the request to be made by the Secretary under section 35AX for the purposes of paragraph 35AB(10)(g). These conditions serve as another limitation to ensure that the actions are computer-related acts and appropriately targeted at responding to the cyber security incident and reflect the specialised skills of the authorised agency which in many circumstances surpass those of the private sector.

82. The things covered by section 35AC are:

- accessing or modifying a computer or computer device that is, or is part of, the asset to which the Ministerial authorisation relates (paragraph (a)) – For example, a specified request may be to access a specified computer prior to undertaking an analysis of it (where analysis is also requested).

- undertaking an analysis of a computer, computer program, computer data or a computer device that is, or is part of, the asset (paragraph (b)) – For example, a specified request may be to undertake analysis of network activity through logs files or server images to identify malicious software (malware).

- if necessary to undertake the analysis under paragraph (b)—install a computer program on a computer that is, or is part of, the asset (paragraph (c)) – For example, a specified request may be to install a specified computer program to run a vulnerability assessment to identify gaps that require patching.

- access, add, restore, copy, alter or delete data held in a computer or a computer device, that is, or is part of, the asset (paragraph (d)) – For example, a specified request may be to identify, access, and delete malware located on a network.

- access, add, restore, copy, alter or delete a computer program that is, or a computer program that is installed on a computer that is, or is part of the asset (paragraphs (e) and (f)) – For example, a specified request may be to restore a program critical to the assets operation that was previously deleted as part of a malicious cyber activity.

- alter the functioning of a computer or a computer device that is, or is part of, the asset (paragraph (g)) – For example, a specified request may be to alter the computer's ability to access a computer network, in order to stop it from infecting other computers.

- remove or disconnect, or connect or add, a computer or a computer device to a computer network that is, or is part of, the asset (paragraphs (h) and (i)) – For example, a specified request may be to disconnect an infected Universal Serial Bus from a computer to mitigate further spread of malware.

- remove a computer or computer device that is, or is part of, the asset from premises (paragraph (j)) – For example, a specified request may be to physically remove a computer from the premises for further analysis (where analysis is also requested).

Section 35AD Consultation

83. New section 35AD of the SOCI Act outlines consultation requirements that must be completed, subject to listed exceptions, by the Minister before issuing a Ministerial authorisation. This consultation requirement ensures that (wherever possible) affected entities are able to inform Government's use of the

powers in Part 3A. The Minister must have regard to any information provided when making a Ministerial authorisation.

84. Subsection (1) provides that, before giving a Ministerial authorisation under paragraphs 35AB(2)(c) or (d) that would enable the Secretary to make an action direction under section 35AQ, the Minister must consult the specified entity unless the delay that would occur in doing so would frustrate the effectiveness of the authorisation.

85. Under subsection (2), before giving an authorisation under paragraphs 35AB(2)(e) or (f) that would enable the Secretary to give an intervention request to the chief executive of the authorised agency, the Minister must:

- if the authorisation is given under paragraph 35AB(2)(e) in relation to a critical infrastructure asset—consult the responsible entity, or entities, for the asset (paragraph (a)), or
- if authorisation is given under paragraph 35AB(2)(f) in relation to a critical infrastructure sector asset—consult the owner/s or operator/s of the asset that the Minister considers most relevant to the authorisation (paragraph (b)).

86. The Minister is not required to undertake the consultation listed in subsection (2) where the delay that would occur in doing so would frustrate the effectiveness of the authorisation.

87. Subsection 35AD(3) requires the Minister, if required to consult under subsections 35AD(1) or (2), to give the entity a copy of the proposed ministerial authorisation and provide the entity 24 hours to make a submission.

88. If consultation is not required under subsection 35AD(1) or (2) then subsection 35AD(3) does not apply. For example, if consultation is not required under subsection 35AD(1) or (2) because consultation would frustrate the effectiveness of the Ministerial authorisation, compliance with subsection 35AD(3) is not required.

89. Consultation with affected entities is vital to ensuring the Minister's decisions are informed and appropriate. In particular, this consultation will assist with satisfying the Minister as to whether an entity is unwilling or unable to take all reasonable steps to respond to the incident (see paragraph 35AB(7)(a) and paragraphs 35AB(10)(b)-(c)). It is also important to provide greater information about the circumstances of the incident to determine whether the proposed course of action is reasonably necessary (see paragraph 35AB(7)(b) and paragraph 35AB(10)(d)), proportionate (see paragraph 35AB(7)(c) and paragraph 35AB(10)(e)) and technically feasible (see paragraph 35AB(7)(d) and paragraph 35AB(10)(f)).

90. However, it is equally important to recognise that due to emergency nature of the regime, in extreme circumstances, compliance with this consultation requirement may impede an effective and timely response to an incident. This is intended to only occur in rare circumstances. For example, the Government may be engaging closely with a particular entity in relation to a cyber security incident involving a particular critical infrastructure asset (Asset 1) and it becomes clear that the malicious actor will imminently gain unauthorised access to another, interconnected, critical infrastructure asset (Asset 2) from the system of Asset 1 and cause catastrophic damage. In such circumstances, the Minister may have sufficient information to determine the

particular action that must occur immediately to prevent the compromise but be unable to undertake the required consultation before the actor compromises Asset 2.

91. Where such rare circumstances occur, the Minister will still need to satisfied of the factors in subsection 35AB(1) as well as subsection 35AB(7) or (10) as relevant. This provides a safeguard by ensuring that the Minister must have sufficient information to form this satisfaction, while allowing for adaptability in the regime. Further, following the making of the authorisation, should the entity bring any concerns to the Minister's attention, subsection 35AH(3) places a duty on the Minister to revoke the authorisation if no longer satisfied of its necessity. Similarly, should the entity raise any concerns with the Secretary which result in the Secretary no longer being satisfied that the Ministerial authorisation is required, subsection 35AH(4) places an obligation on the Secretary to inform the Minister as soon as practicable. This ensures that any consultation that occurs after the Ministerial authorisation is made can be used to inform its continuation or potential revocation.

92. As responsible entities have not been identified in the legislation in relation to critical infrastructure sectors assets, due to this being a significantly broader class of assets, the Minister must exercise discretion as to who is the most relevant entity to consult with in relation to the Ministerial authorisation. An owner or operator, or both, may be considered relevant if the Ministerial authorisation will directly affect them or affect an aspect of the asset for which they are responsible. This flexibility will allow for the most appropriate entity or entities to be provided with the opportunity to make representations to the Minister in relation to the proposed authorisation.

Section 35AE Form and notification of Ministerial authorisation

93. New section 35AE of the SOCI Act outlines the permitted forms of a Ministerial authorisation given under subsection 35AB(2), and the requirements to notify relevant entities and other stakeholders about the authorisation being given.

94. Subsection (1) provides that a Ministerial authorisation may be given orally or in writing. However, an authorisation must not be given orally unless the delay that would occur if the authorisation were to be made in writing would frustrate the effectiveness of any directions that may be given under sections 35AK and 35AQ, or any requests that may be given under section 35AX (see subsection (2)).

Subsections 35AE(3)-(5)—Notification of Ministerial authorisations given orally

95. Under subsection (3), if a Ministerial authorisation is given orally, the Minister must make a written record of the authorisation and give a copy of the written record to the Secretary and the IGIS within 48 hours of giving the authorisation. This will ensure there are accurate records of the authorisation. The notification of the IGIS is important to ensure that the Inspector-General has an opportunity to consider whether to exercise any of their oversight powers in relation to the Ministerial authorisation, or actions taken in response to it.

96. Subsection (4) provides that, if a Ministerial authorisation is given orally and relates to a critical infrastructure asset, the Minister must also give a copy of a written record of the authorisation to the responsible entity for the asset within 48 hours of giving the authorisation. In addition, under subsection (5), if a Ministerial authorisation is given orally and relates to a critical infrastructure sector asset that is not a

critical infrastructure asset, the Minister must also give a copy of the written record of the authorisation to the most relevant owner/s or operator/s of the asset. These requirements mean that the affected entity is provided with a written copy of the authorisation. This is an important safeguard to ensure the entity has a clear understanding of the extent of the authorisation.

Subsections 35AB(6)-(8)—Notification of Ministerial authorisations given in writing

97. Under subsection (6), if a Ministerial authorisation is given in writing, the Minister must give a copy of the authorisation to the Secretary and the IGIS within 48 hours of giving the authorisation. The notification of the IGIS is important to ensure that the Inspector-General has an opportunity to consider whether to exercise any of their oversight powers in relation to the Ministerial authorisation, or actions taken in response to it.

98. Subsection (7) provides that, if a Ministerial authorisation is given in writing and relates to a critical infrastructure asset, the Minister must also give a copy of the Ministerial authorisation to the responsible entity for the asset within 48 hours of giving the authorisation. In addition, under subsection (8), if a Ministerial authorisation is given in writing and relates to a critical infrastructure sector asset that is not a critical infrastructure asset, the Minister must also give a copy of the Ministerial authorisation to the most relevant owner/s or operator/s of the asset. These requirements mean that the affected entity is provided with a written copy of the authorisation. This is an important safeguard to ensure the entity has a clear understanding of the extent of the authorisation.

Section 35AF Form of application for Ministerial authorisation

99. Subsection 35AB(2) of the SOCI Act (outlined above) provides that the Minister may make a Ministerial authorisation on application by the Secretary. New section 35AF of the SOCI Act outlines requirements for the making of an application by the Secretary for the purpose of subsection 35AB(2).

100. Subsection (1) provides that the Secretary may make the application orally or in writing. Subsection (2) provides that the Secretary must not make an oral request for a Ministerial authorisation unless the delay that would occur, should the application be made in writing, would frustrate the effectiveness of any directions that may be given by the Secretary under sections 35AK or 35AQ, or any requests given under section 35AX.

101. Under subsection (3), if a request for a Ministerial authorisation is made orally, the Secretary is required to make a written record of the application and give a copy of the written record to the Minister within 48 hours of making the application.

102. It is noted that any written request is already required to be given to the Minister under subsection 35AB(2) above.

Section 35AG Duration of Ministerial authorisation

103. New section 35AG of the SOCI Act sets out the duration of a Ministerial authorisation given under subsection 35AB(2).

Subsection 35AG(1)—Scope

104. Subsection (1) provides that section 35AG applies to a Ministerial authorisation given in relation to a cyber security incident and an asset. This is intended to cover all types of Ministerial authorisations that may be given under subsection 35AB(2).

Subsection 35AG(2)—Duration of Ministerial authorisation

105. Subsection (2) provides that, subject to this section, the Ministerial authorisation remains in force for the period specified in the Ministerial authorisation which must not exceed 20 days. That is, the duration of the Ministerial authorisation is to be included in the authorisation itself and can be for any period up to and including 20 days.

106. Although it is recognised that the comprehensive resolution of a serious cyber security incident is likely to take longer than 20 days, this maximum timeframe is intended to reflect the emergency nature of the intervention. This regime is only intended to be used as a last resort to achieve outcomes that are considered necessary in light of the severity of the impact to the nation and for no longer than strictly necessary. It is noted that subsection 35AH(3) requires the Minister to revoke an authorisation if satisfied that it is no longer required, further ensuring that the authorisation does not continue for any longer than necessary.

Subsection 35AG(3)-(5)—Fresh Ministerial authorisations

107. Under subsection (3), if a Ministerial authorisation is in force, the SOCI Act does not prevent the Minister from giving a further fresh Ministerial authorisation that is in the same, or substantially the same, terms as the original authorisation and that comes into force immediately after the expiry of the original authorisation.

108. In deciding whether to give a fresh Ministerial authorisation in accordance with subsection (3), in addition to the various factors the Minister must be satisfied of in section 35AB, the Minister must also have regard to the number of occasions on which Ministerial authorisations have been made in relation to the incident and the asset (under subsection (4)). Subsection (5) clarifies that subsection (4) does not, however, limit the matters to which the Minister may have regard to in deciding whether to give a fresh Ministerial authorisation.

109. These subsections are intended to allow the Minister, if satisfied that a Ministerial authorisation continues to be required, to make a fresh authorisation. However, in making a further authorisation, the Minister must meet all the requirements that would ordinarily be required in relation to the making of a Ministerial authorisation, in addition to having regard to the extra consideration in subsection (4).

Section 35AH Revocation of Ministerial authorisation

110. New section 35AH of the SOCI Act sets out how a Ministerial authorisation given under subsection 35AB(2) can be revoked.

Subsection 35AH(1)—Scope

111. Subsection (1) provides that section 35AH applies to a Ministerial authorisation that is in force in relation to a cyber security incident and an asset. This is intended to cover all types of Ministerial authorisations that may be given under subsection 35AB(2).

Subsection 35AH(2)—Power to revoke Ministerial authorisation

112. Subsection (2) provides that the Minister may, in writing, revoke a Ministerial authorisation. The revocation must be made in writing, and cannot be done orally.

Subsections 35AH(3)-(4)—Duty to revoke Ministerial authorisation

113. Under subsection (3), if the Minister is satisfied that the Ministerial authorisation is no longer required to respond to the cyber security incident concerned, the Minister must, in writing, revoke the authorisation.

114. Subsection (4) further provides that, if the Secretary is satisfied that the Ministerial authorisation is no longer required to respond to the cyber security incident, the Secretary must notify the Minister that the Secretary is so satisfied and do so as soon as practicable after the Secretary becomes so satisfied. This notification will cause the Minister to reconsider the Ministerial authorisation, and if no longer satisfied that it is required, subsection (3) would require it to be revoked.

Subsections 35AH(5)-(7)—Notification of revocation

115. Subsection (5) provides that, if any Ministerial authorisation is revoked, the Minister must give a copy of the revocation to the Secretary, the IGIS and each relevant entity to which the authorisation relates within 48 hours of the revocation.

116. Under subsection (6), if the revocation relates to a critical infrastructure asset, the Minister must also give a copy of the revocation to the responsible entity for the asset. Subsection (7) further provides that, if the revocation relates to a critical infrastructure sector asset that is not a critical infrastructure asset, the Minister must also give a copy of the revocation to the owner or operator of the asset the Minister considers to be most relevant.

Subsection 35AH(8)—Revocation is not a legislative instrument

117. Subsection (8) clarifies that a revocation of a Ministerial authorisation is not a legislative instrument. This is reasonable in these circumstances because:

- the public disclosure of the authorisation may reveal weakness or vulnerabilities in critical infrastructure assets that could be exploited by nefarious actors or otherwise cause damage in relation to the asset.
- the authorisation applies the law in a particular circumstance to particular facts, and does not determine or alter the content of the law for the purposes of subsection 8(4) of the Legislation Act.

Subsection 35AH(9)—Application of Acts Interpretation Act 1901

118. Subsection (9) provides that section 35AH does not, by implication, affect the application of subsection 33(3) of the Acts Interpretation Act to an instrument made under a provision of the SOCI Act (other than Part 3A).

Section 35AJ Minister to exercise powers personally

119. New section 35AJ of the SOCI Act provides that the power of the Minister under Division 2 of Part 3A (in particular under subsection 35AB(2) to give a Ministerial authorisation) may only be exercised by the Minister personally and cannot be delegated on an implied basis, noting that there is no express provision enabling delegation of the Minister's powers in the SOCI Act or included the Bill. Given the serious nature of the powers in Part 3A, it is reasonable and appropriate to require these powers to be exercised personally by the elected official with responsibility for ensuring the security of Australia's critical infrastructure.

Division 3—Information gathering directions

120. New Division 3 of Part 3A of the SOCI Act provides for the Secretary, when authorised to do so by the Minister, to give directions to entities to provide information to the Secretary.

Section 35AK Information gathering direction

121. New section 35AK of the SOCI Act sets out when the Secretary may give an information gathering direction.

Subsection 35AK(1)—Scope

122. Subsection (1) provides that section 35AK applies if a Ministerial authorisation has been given under paragraphs 35AB(2)(a) or (b) in relation to a cyber security incident and an asset.

Subsections 35AK(2)-(6)—Direction

123. Subsection (2) applies where an entity is a relevant entity for the asset to which the Ministerial authorisation relates and the Secretary has reason to believe that the entity has information that may assist with determining whether a power under this Act should be exercised in relation to the incident and the asset. In these circumstances, the Secretary may direct the entity to:

- give any such information to the Secretary (paragraph (c)), and
- do so within the period, and in the manner, specified in the direction (paragraph (d)).

124. An effective and appropriate response to a serious cyber security incident requires a strong understanding of the nature and extent of the incident, as well as a strong understanding of the circumstances of the asset including its cyber security maturity, its vulnerabilities and its interdependencies. This information will inform any decisions in relation to further Ministerial authorisations, and be important in ensuring that those Ministerial authorisations are reasonably necessary and proportionate.

125. A direction under subsection (2) may be given under a Ministerial authorisation given under paragraphs 35AB(2)(a) or (b). These types of Ministerial authorisations differ from other types outlined in

paragraphs 35AB(2)(c) to (f). In particular, Ministerial authorisations given under paragraphs 35AB(2)(a) and (b) provide a level of discretion to the Secretary to determine the content of the Secretary's directions under subsection (2), as well as allowing multiple directions to be made, subject to the conditions set out in section 35AK. By comparison, Ministerial authorisations given under 35AB(2)(c) to (f) only permit the Secretary to make directions or requests that are explicitly authorised by the Minister.

126. This flexibility in relation to information gathering directions reflects the fact that the relevant directions that can be made under subsection (2) are less invasive than the types of directions that can be given under the Ministerial authorisations to which paragraphs 35AB(2)(c) to (f) relate, and that information gathering can be an iterative process and therefore administrative flexibility is required to achieve an effective outcome. The information provided in response to one direction may raise the need for further information to be provided, precipitating a further direction to be given by the Secretary under the same Ministerial authorisation. For example, the information reveals that a particular part of a computer network has been compromised and to assist in determining whether a Ministerial authorisation is required for an action direction, the Secretary first needs to know the purpose and significance of that part of the system and any mitigation measures in place.

127. Under subsection (3), the period specified in the direction under paragraph (2)(d) must end at or before the end of the period for which the Ministerial authorisation is in force—noting that the authorisation can be in force for a specified period not exceeding 20 days (subsection 35AG(2)).

128. Subsections (4) and (5) provide further limitations on the giving of directions under subsection (2). Subsection (4) provides that the Secretary must not give the direction under subsection (2) unless the Secretary is satisfied that the direction is a proportionate means of obtaining the information (paragraph (a)) and compliance with the direction be the entity is technically feasible (paragraph (b)).

129. The proportionality test at paragraph (4)(a) is intended to ensure the Secretary considers whether the information can be obtained through other less invasive avenues, and whether the value of the information to assisting with determining whether a power under the Act should be exercised is proportionate to the nature of the request.

130. The requirement for directions to be technically feasible under paragraph (4)(b) is a further limitation on the information gathering directions that can be issued by the Secretary. A direction is technically feasible when the direction relates to a course of action that is reasonably possible to execute, or within the existing capability of the relevant entity. A direction is considered not to be technically feasible if there is no technical capability that could be utilised to produce the outcome that is sought. For example, a direction to produce a data set that does not exist, and cannot technically be generated, would not be regarded as technically capable.

131. The consultation requirement at subsection (6) ensures that the affected entities are afforded an opportunity to provide meaningful advice and guidance to the Secretary when determining the proportionality and technical feasibility of a direction. However, this consultation requirement does not apply if the delay that would occur in complying with the requirement would frustrate the effectiveness of the direction.

132. In addition, subsection (5) provides a further limitation on the directions that the Secretary can give under this section to ensure they are reasonable and appropriate. Subsection (5) provides that the Secretary must not give a direction that would require the entity to:

- do an act or thing that would be prohibited by sections 7 or 108 of the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) (paragraphs (a) and (b)), or
- do an act or thing that would, disregarding the SOCI Act, be prohibited by sections 276, 277 or 278 of the Telecommunications Act (paragraph (c)).

133. The TIA Act and the Telecommunications Act, respectively, provide specific protections for telecommunications data, including stored communications and data relating to the provision of carriage services, and for that data only to be accessible where the specific authorisation provisions in those Acts are available. The intention of subsection (5) of this section is to ensure that a direction given by the Secretary under subsection (2) does not enable the Secretary to collect such telecommunications data. Should this information be required, the dedicated mechanisms provided in the TIA Act and Telecommunications Act would need to be used. This regime is not to be used as an alternative pathway to access those forms of information.

Subsection 35AK(7)—Other powers not limited

134. Subsection (7) provides that section 35AK does not, by implication, limit a power conferred by another provision of the SOCI Act. This ensures that the other powers in the SOCI Act, such as the Secretary's information gathering powers at existing section 37, in the Act are not taken to be limited as a result of this power. It is important to note that the Secretary's powers under section 37 are limited to a reporting entity for, or an operator of, a critical infrastructure asset, while a Ministerial authorisation made under paragraph 35AB(2)(b) may extend to a relevant entity for a critical infrastructure sector asset.

Section 35AL Form of direction

135. New section 35AL of the SOCI Act provides that a direction from the Secretary under section 35AK may be given orally or in writing (see subsection (1)). Under subsection (2), the Secretary must not give a direction orally unless the delay that would result from doing in writing would frustrate the effectiveness of the direction. Under subsection (3), if the Secretary gives a direction orally, the Secretary must make a written record of the direction and give a copy of the written record to the entity to which the direction relates within 48 hours of the direction being given.

Section 35AM Compliance with an information gathering direction

136. New section 35AM of the SOCI Act requires an entity to comply with a direction given to the entity under section 35AK to the extent that the entity is capable of doing so. That an entity will not be in breach of this obligation if they are not capable of complying is important to accommodate, for example, for situations where consultation has not been able to occur (see subsection 35AK(6)) and therefore the entity was not able to inform the Secretary that compliance would not be technically feasible.

137. Breach of this obligation is subject to a civil penalty of up to 150 penalty units. This penalty is a proportionate response based on the nature of the infringement and is designed to deter non-compliance with an information gathering direction. This penalty is commensurate with the non-compliance for an obligation to comply with directions under the ATSA and MTOFSA. The penalty reflects the importance of enabling government to obtain information relevant to the prevention of, mitigation of or restoration from a serious cyber security incident in a timely and effective manner.

Section 35AN Self-incrimination etc.

138. New section 35AN of the SOCI Act provides that:

- an entity is not excused from giving information under section 35AK (as required under section 35AM) on the ground that the information might tend to incriminate the entity (subsection (1)), and
- if an individual would ordinarily be able to claim the privilege against self-exposure to a penalty in relation to giving information under section 35AK, the individual is not excused from giving information under that section on that ground (subsection (2)).

139. A note to subsection (2) indicates that a body corporate is not entitled to claim the privilege against self-exposure to penalty.

140. This provision highlights that the importance of the information being sought to provide the necessary understanding to support Government's decisions as to the necessary actions to respond to a serious cyber security incident. The information is not intended to be used for a compliance purpose (as reflected by section 35AP) and it is crucial that timely and accurate information is provided to prevent further prejudice to Australia's national interests.

Section 35AP Admissibility of information etc.

141. New section 35AP of the SOCI Act limits how information given to the Secretary under a section 35AK direction can be admitted into evidence. This provides important protections for the entity noting that section 35AN abrogates their ordinary rights in relation to self incrimination and exposure to penalty. Under this section, such information is not admissible in evidence against an entity:

- in criminal proceedings other than proceedings for an offence against section 137.1 and 137.2 of the *Criminal Code*, which relate to providing false and misleading statements and documents to the Commonwealth, that relate to the SOCI Act (paragraph (c)), and
- in civil proceedings other than proceedings for a recovery of a penalty in relation to a contravention of section 35AM (paragraph (d)).

142. When read together, sections 35AN and 35AP facilitate open and transparent information gathering to support the operation of the Part in emergencies, while guaranteeing that the information provided by the entity cannot later be admitted as evidence in a proceeding against the court except in relation to failing to comply with the direction, or doing so in a false or misleading manner.

143. This provision is important to encourage open and accurate reporting noting the importance of the information being provided, however equally balances the impact of new section 35AN to ensure that the information provided is not used against the individual as evidence. This position reflects that this information is not being sought for a compliance purpose but rather protect critical infrastructure in an emergency.

Division 4—Action directions

144. New Division 4 of Part 3A of the SOCI Act provides for the Secretary, when authorised to do so by the Minister, to give directions to relevant entities to take, or refrain from taking, certain actions in the circumstances outlined below.

Section 35AQ Action direction

145. New section 35AQ of the SOCI Act provides that the Secretary may, pursuant to a Ministerial authorisation, give the relevant entity for a critical infrastructure asset or a critical infrastructure sector asset a direction that directs the entity to do, or refrain from doing, a specified act or thing within the period specified in the direction (see subsection (1)).

146. Under subsection (2), the Secretary must not give a direction under section 35AQ unless the direction:

- is identical to a direction specified in a Ministerial authorisation under paragraphs 35AB(2)(c) or (d) (paragraph (a))
- includes a statement to the effect that the direction is authorised by the Ministerial authorisation (paragraph (b)), and
- specifies the date on which the Ministerial authorisation was given (paragraph (c)).

147. The effect of paragraph 35AQ(2)(a) is that the Secretary actions the direction that is authorised by the Minister.

148. A note to subsection (2) reminds the reader that a Ministerial authorisation must not be given unless, amongst other things, the Minister is satisfied that the direction is reasonably necessary for the purposes of responding to a cyber security incident, as outlined under section 35AB above (see paragraph 35AB(7)(b) in particular).

149. Subsection (3) provides that the period specified in the direction as required under paragraph (2)(c) must end at or before the end of the period for which the Ministerial authorisation is in force— noting that the authorisation can be in force for a period no longer than 20 days under subsection 35AG(2). The intention of this provision is to clarify that a direction authorised under a Ministerial authorisation cannot extend beyond the authorisation itself. This reflects that the direction is the operationalising of the authorisation.

150. Subsection (4) provides that a direction under section 35AQ is subject to such conditions, if any, as are specified in the direction. This provides flexibility and ensures any direction can be narrowed to reflect the unique circumstances of the incident.

151. Under subsection (5), the Secretary must not give a direction under section 35AQ that would require an entity to give information to the Secretary. The more appropriate mechanism to require information to be provided are the information gathering directions under Division 2 of Part 3A of the SOCI Act, as outlined above. That mechanism has been designed for that express purpose and has tailored and proportionate safeguards, and therefore should be the mechanism used to gather information should it be required.

Subsection 35AQ(6)—Other powers not limited

152. Subsection (6) provides that section 35AQ does not, by implication, limit a power conferred by another provision of the SOCI Act.

Section 35AR Form of direction

153. New section 35AR of the SOCI Act provides that a direction given by the Secretary under section 35AQ may be given orally or in writing (subsection (1)). Under subsection (2), the Secretary must not, however, give a direction orally unless the delay that would result from doing in writing would frustrate the effectiveness of the direction. Under subsection (3), if the Secretary gives a direction orally, the Secretary must make a written record of the direction and give a copy of the written record to the entity to which the direction relates within 48 hours of the direction being given.

Section 35AS Revocation of direction

154. New section 35AS of the SOCI Act sets out how a direction given by the Secretary under section 35AQ is revoked.

Subsection 35AS(1)—Scope

155. Subsection (1) provides that section 35AS applies if a direction is in force under section 35AQ in relation to a Ministerial authorisation (given under paragraphs 35AB(2)(c) or (d)) and the direction was given to a particular entity.

Subsection 35AS(2)—Power to revoke direction

156. Subsection (2) provides that the Secretary may, by written notice given to the entity, revoke the direction. This means that the Secretary may elect to revoke the direction should the Secretary consider that it is no longer appropriate (see in particular subsection 35AS(3)).

Subsection 35AS(3)—Duty to revoke direction

157. Under subsection (3), if the Secretary is satisfied that the direction is no longer required to respond to the cyber security incident to which the Ministerial authorisation relates, the Secretary must, by written notice given to the entity, revoke the direction. This is an important safeguard to ensure that the direction is not in place for any longer than strictly necessary. It also ensures that, should continued engagement with the entity reveal new information which changes the need for the direction, or the circumstances themselves change which render the direction to be no longer necessary, the Secretary has a duty to revoke the direction.

For example, if the direction relates to deleting a computer program and, as a result of unauthorised activity, that program is already deleted, upon learning of this, the Secretary may revoke the direction.

Subsection 35AS(4)—Automatic revocation of direction

158. Subsection (4) provides that, if the Ministerial authorisation ceases to be in force (either by expiration of the duration of the authorisation under subsection 35AG(2) or revocation under section 35AH), the direction is automatically revoked. As the direction is operationalising the authorisation, the termination of the authorisation appropriately triggers the termination of the direction to ensure that no unauthorised action occurs.

Subsection 35AS(5)—Application of Acts Interpretation Act 1901

159. Subsection (5) provides that section 35AS does not, by implication, limit a power conferred by another provision of the SOCI Act.

Section 35AT Compliance with direction

160. New section 35AT of the SOCI Act provides that an entity commits an offence if all of the following apply:

- the entity is given a direction by the Secretary under section 35AQ (paragraph (a))
- the entity engages in conduct after receiving the direction (paragraph (b)), and
- the entity's conduct breaches the direction (paragraph (c)).

161. Subsection (1) provides that the offence does not apply if the entity took all reasonable steps to comply with the direction. This is intended to ensure that the entity is not liable for failing to comply with the direction when compliance is not technically possible, for example due to an unforeseen lack of capability, or due to changing circumstances. For example if a direction provides that the entity must alter the configuration settings on a computer program, and before they can do so, the malicious actor renders the computer, on which the program sits, inaccessible making compliance impossible. However, this subsection is not intended to provide an avenue to excuse unwillingness to comply with the direction.

162. The penalty for this offence is imprisonment for 2 years or 120 penalty units, or both. If the entity who commits the offence is a corporation, the penalty will be 600 penalty units by application of subsection 4B(3) of the Crimes Act. This penalty is a proportionate response based on the nature of the conduct and is designed to deter non-compliance with an action direction. This penalty is commensurate with the offence of obstruction of Commonwealth public officials at section 149.1 of the Criminal Code. This offence has a similar purpose to section 149.1 of the Criminal Code and the penalty reflects the significance of the circumstances that led to the direction being issued, and the potential prejudice to Australia's national interest should it not be complied with.

Section 35AV Directions prevail over inconsistent obligations

163. New section 35AV of the SOCI Act provides that, if an obligation under the SOCI Act is applicable to an entity, the obligation has no effect to the extent to which it is inconsistent with a direction given to the

entity by the Secretary under section 35AQ. This provision ensures that any action required under section 35AQ takes precedence over any potential contradictory requirements under other parts of the SOCI framework. The primacy of the directions reflect that an appropriate response to an emergency may warrant a deviation from the other obligations contained in the Act.

Section 35AW Liability

164. New section 35AW of the SOCI Act provides that:

- an entity is not liable to an action or other proceedings for damages for or in relation to an act done or omitted in good faith in compliance with a direction given under section 35AQ (subsection (1)), and
- an officer, employee or agent of an entity is not liable to an action or other proceedings for damages for or in relation to an act done or omitted in good faith in connection with an act done or omitted by the entity as mentioned in subsection (1) (subsection (2)).

165. This ensures that relevant entities, when acting in response to a compulsory legal direction, are not subjected to civil liabilities. The absence of such an immunity would result in the entity being forced to choose between complying with the lawful direction or for example, contractual obligations. Noting the objectives of the directions are to respond to a serious cyber security incident that poses a material risk of serious prejudice to Australia's national interests, it is important that there are no barriers to the entity complying with such a direction and that they are not penalised for doing so. For example, a direction may require the entity, or its representatives, to temporarily disable customers' access to a particular system as that portal is being exploited by the malicious actor and needs to be reconfigured to uplift the security. Compliance with such a direction may breach contractual arrangements the entity, or its representatives, have with their customers in relation to continuity of service.

Division 5—Intervention requests

166. New Division 5 of Part 3A of the SOCI Act provides for the Secretary, when authorised to do so by the Minister, to make requests to the chief executive of the authorised agency.

Section 35AX Intervention request

167. New section 35AX of the SOCI Act empowers the Secretary to give the chief executive of the authorised agency a request that the authorised agency do one or more specified acts or things within the period specified in the request (see subsection (1)). The chief executive of the authorised agency is defined in section 5 to mean the Director-General of ASD.

168. Subsection (2) provides that the Secretary must not give a request under subsection (1) unless the request:

- is identical to a request specified in a Ministerial authorisation under paragraph 35AB(2)(e) or (f) (paragraph (a))

- includes a statement to the effect that the request is authorised by the Ministerial authorisation (paragraph (b)), and

- specifies the date on which the Ministerial authorisation was given (paragraph (c)).

169. A note to subsection (2) reminds the reader that a Ministerial authorisation must not be given unless, amongst other things, the Minister is satisfied that the request is reasonably necessary for the purposes of responding to a cyber security incident, as outlined under section 35AB above (see paragraph 35AB(10)(d) in particular).

170. Subsection (3) provides that the period specified in the request as required under subsection (2)(c) must end at or before the end of the period for which the Ministerial authorisation is in force— noting that the authorisation can be in force for a period no longer than 20 days under subsection 35AG(2). The intention of this provision is to clarify that a request authorised under a Ministerial authorisation cannot extend beyond the authorisation itself. This reflects that the request is the operationalising of the authorisation.

171. Subsection (4) provides that a request under section 35AX is subject to such conditions, if any, as are specified in the request. This provides flexibility and ensures any direction can be narrowed to reflect the unique circumstances of the incident.

172. Subsection (5) provides that a request made by the Secretary does not extend to:

- doing an act or thing that would be prohibited by sections 7 or 108 of the TIA Act (paragraphs (a) and (b)), or

- doing an act or thing that would, disregarding the SOCI Act, be prohibited by sections 276, 277 or 278 of the Telecommunications Act (paragraph (c)).

173. The TIA Act and the Telecommunications Act, respectively, provide specific protections for telecommunications data, including stored communications and data relating to the provision of carriage services, and for that data only to be accessible where the specific authorisation provisions in those Acts are available. The intention of subsection (5) of this section is to ensure that a request given by the Secretary under subsection (2) does not enable the authorised agency to collect such telecommunications data. Should this information be required, the dedicated mechanisms provided in the TIA Act and Telecommunications Act would need to be used. This regime is not to be used as an alternative pathway to access those forms of information.

Subsection 35AX(6)—Other powers not limited

174. Subsection (6) provides that section 35AX does not, by implication, limit a power conferred by another provision of the SOCI Act.

Section 35AY Form and notification of request

175. New section 35AY of the SOCI Act provides that a request under section 35AX may be given orally or in writing (see subsection (1)). The Secretary must not, however, give a section 35AX request orally unless the delay that would result from doing in writing would frustrate the effectiveness of the request (subsection (2)). Under subsection (3), if the Secretary gives a direction orally, the Secretary must make a written record of the request and give a copy of the written record of the request to the chief executive of the authorised agency within 48 hours of the request being given.

Subsections 35AY(3)-(5)—Notification of requests given orally

176. Subsection (3) requires the Secretary, if a request is given orally, to make a written record of the request and give a copy of the written record of the request to the chief executive of the authorised agency within 48 hours of giving the request.

177. If a request is given orally in relation to a critical infrastructure asset, under subsection (4), the Secretary must give a written record of the request to the responsible entity for that asset within 48 hours of giving the request. Alternatively, under subsection (5), if a request is given orally in relation to a critical infrastructure sector asset that is not a critical infrastructure asset, the Secretary must also give a written record of the request to the owner/s or operator/s of that asset that the Secretary considers to be most relevant to the request. These obligations will ensure that affected entities have sufficient visibility of the exact scope of the request. Should the entity consider that the approved staff member of the authorised agency, when acting in response to the request exceeds the scope of the request, the entity will be able to make a complaint to the Inspector-General of Intelligence and Security.

Subsections 35AY(6)-(8)—Notification of requests given in writing

178. Subsection (6) requires the Secretary to provide a copy of a written request under section 35AX to the chief executive of the authorised agency within 48 hours of making the request.

179. If a request is given in writing in relation to a critical infrastructure asset, under subsection (7), the Secretary must give a written record of the request to the responsible entity for that asset within 48 hours. In addition, under subsection (8), if a request is given in relation to a critical infrastructure sector asset that is not a critical infrastructure asset, the Secretary must give a written record of the request to the owner/s or operator/s of that asset that the Secretary considers to be most relevant to the request within 48 hours.

Section 35AZ Compliance with request

180. New section 35AZ of the SOCI Act is intended to clarify that the authorised agency is authorised to do an act or thing in compliance with a request under section 35AX (see subsection (1)). This provisions clarifies that the authorised agency has lawful authority to do acts or things in compliance with a request.

181. Subsection (2) is a deeming provision, which provides that an act or thing done by the authorised agency in compliance with a request under section 35AX is taken to be done in the performance of the function conferred on the authorised agency by paragraph 7(1)(f) of the Intelligence Services Act, which provides that it is a function of ASD to cooperate with and assist bodies referred to in section 13A in accordance with that section.

182. Section 13A of the Intelligence Services Act provides that an agency governed by the Act may cooperate with and assist the bodies listed in subsection 13A(1) in the performance of their functions, subject to any arrangements made or directions given by the responsible Minister for that agency (paragraph 13A(2)(a)) and upon request from the head of the body (paragraph 13A(2)(b)). Paragraph 13A(1)(c) lists a Commonwealth authority, or a State authority, that is prescribed by the regulations for the purpose of that paragraph as a body that an agency may cooperate with and assist. It is proposed that the Home Affairs Department, being the Department administered by the Minister administering the SOCI Act, will be prescribed in regulations on or before the commencement of the Bill—meaning that it is possible for ASD to have the function of cooperating and assisting the Department of Home Affairs.

183. The effect of subsection (2) is that any activities done by ASD in relation to a request from the Secretary under section 35AX will be within the existing functions of ASD for the purposes of the Intelligence Services Act.

Section 35BA Revocation of request

184. New section 35BA of the SOCI Act sets out the circumstances in which a request under section 35AX is revoked.

Subsection 35BA(1)—Scope

185. Subsection (1) provides that section 35BA applies if a request is in force under section 35AX in relation to a Ministerial authorisation (given under paragraphs 35AB(2)(e) or (f)).

Subsection 35BA(2)—Power to revoke request

186. Subsection (2) provides that the Secretary may, by written notice given to the chief executive of the authorised agency, revoke the request.

Subsection 35BA(3)—Duty to revoke request

187. Under subsection (3), if the Secretary is satisfied that the request is no longer required to respond to the cyber security incident to which the Ministerial authorisation relates, the Secretary must, by written notice given to the entity, revoke the request.

188. Under subsection (3), if the Secretary is satisfied that the request is no longer required to respond to the cyber security incident to which the Ministerial authorisation relates, the Secretary must, by written notice given to the chief executive of the authorised agency, revoke the request. This is an important safeguard to ensure that the request is not in place for any longer than strictly necessary. It also ensures that, should continued engagement with the entity reveal new information which changes the need for the request, or the circumstances themselves change which render the direction to be no longer necessary, the Secretary has a duty to revoke the request. For example, if the entity advises, and the Secretary is satisfied, that the entity has been able to take all reasonable necessary steps to respond to the incident the Secretary must revoke the request.

Subsection 35BA(4)—Automatic revocation of direction

189. Subsection (4) provides that, if the Ministerial authorisation ceases to be in force (either by expiration of the duration of the authorisation under subsection 35AG(2) or revocation under section 35AH), the request is automatically revoked. As the request is operationalising the authorisation, the termination of the authorisation appropriately triggers the termination of the request to ensure that no unauthorised actions occur.

Subsection 53BA(5)—Notification of revocation of request

190. Under subsection (5), if a request under section 35AX is revoked by the Secretary, the Secretary must give a copy of the revocation to the chief executive of the authorised agency and each relevant entity for the asset as soon as practicable after the revocation.

Subsection 35BA(6)—Application of Acts Interpretation Act 1901

191. Subsection (6) provides that section 35BA does not, by implication, affect the application of subsection 33(3) of the Acts Interpretation Act 1901, other than a provision under Part 3A of the SOCI Act.

Section 35BB Relevant entity to assist the authorised agency

192. New section 35BB of the SOCI Act makes it a requirement for an entity to assist the authorised agency for the purposes of complying with the request made by the Secretary under section 35AX.

193. Under subsection (1), if a request under section 35AX is in force in relation to a critical infrastructure asset or a critical infrastructure sector asset and the entity is a relevant entity for the asset, then an approved staff member of the authorised agency may require the entity to:

- provide the approved staff member with access to the premises for the purpose of the authorised agency complying with the request (paragraph (c)), or
- provide the authorised agency with specified information or assistance that is reasonably necessary to allow the authorised agency to comply with the request (paragraph (d)).

194. Paragraph (1)(c) is intended to ensure that the cooperation of the entity is sought to facilitate access to the premises as required to comply with the request, for example, prior to any force being used.

195. Paragraph (1)(d) is required to ensure that the authorised agency can obtain any necessary incidental information and assistance to assist them in complying with the request. This is crucial to prevent any unintended consequences that may otherwise occur which would be contrary to the purpose of the request. In taking the actions set out in the request, the authorised agency may need to seek the assistance of the entity to understand the most effective and appropriate way to, for example, execute a computer program or locate the relevant data. This will assist the entity from unintended consequences or unnecessary actions. The information and assistance that can be request must be reasonably necessary to comply with the request, ensuring that this obligation is strictly limited to facilitating compliance and cannot be used for any alternative purposes.

196. A note to subsection (1) directs the reader of the legislation to also see section 149.1 of the *Criminal Code*, which deals with obstructing and hindering Commonwealth public officials, which includes approved staff members of the authorised agency. Failing to comply with a requirement under this sector may amount to a criminal offence under that provision of the Criminal Code.

197. Subsection (2) provides that a staff member of the authorised agency cannot require the entity to provide the approved staff member with access to premises under paragraph (1)(c) where the premises is used solely or primarily as a residence. This limitation is intended to ensure no undue invasion of personal privacy. Should these powers be required to be used, the focus is likely to be on the premises of large corporate entities where the relevant asset is located.

198. Subsection (3) provides that an entity must comply with a requirement under subsection (1). Breach of this obligation is subject to a civil penalty of up to 150 penalty units. This penalty is a proportionate response based on the nature of the infringement and is designed to deter non-compliance with a requirement for an entity to assist an authorised agency to do an act or thing in compliance with an intervention request. The penalty reflects the significance of the circumstances that led to the request being made, and the potential prejudice to Australia's national interest should the entity not provide the necessary incidental assistance to the authorised agency to allow for the request to be complied with.

199. Subsection (4) provides that an entity is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith in compliance with subsection (1).

200. Subsection (5) provides that an officer, employee or agent of an entity is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith in connection with an act done or omitted by the entity as mentioned in subsection (4).

201. These protections ensure that the entity, and its officers, employees or agents, are able to fully cooperate with the approved staff member in responding to the incident.

Section 35BC Constable may assist the authorised agency

202. New section 35BC of the SOCI Act provides that, if an entity refuses or fails to provide a staff member of the authorised agency with access to premises when required to do so under subsection 35BB(1) then:

- the approved staff member may enter the premises for the purpose of the authorised agency complying with the relevant section 35AX request (paragraph (1)(a)), and
- a constable may assist the approved staff member in gaining access to the premises using reasonable force against property (subparagraph (1)(b)(i)) and if necessary to assist, enter the premises (subparagraph (1)(b)(ii)).

203. Subsection (2) provides that, if an approved staff member of the authorised agency has entered premises for the purpose of complying with a request under section 35AX, a constable may:

- assist the authorised agency in complying with the request by using reasonable force against property located on the premises (paragraph (a)), and

- enter the premises for this purpose (paragraph (b)).

204. Constable is defined to have the same meaning given by the Crimes Act. This means that a member or special member of the Australian Federal Police, or a member of a police force of a State or Territory, is able to use force to enter premises in limited circumstances, or to assist the authorised agency in complying with the section 35AX request, under these provisions. Constables are trained in the use of force against property and are subject to various oversight regimes, for example, the Australian Federal Police is subject to oversight by the Commonwealth Ombudsman. An entity will be permitted to make a complaint to the Commonwealth Ombudsman in relation to any concerns with the operation of the powers.

205. It is reasonable and proportionate to permit a constable to use force for the express and strictly limited purpose of assisting the authorised agency with fulfilling an intervention request noting the likely ramification to Australia's national interest if the cyber security incident is not addressed. The constable would be permitted to use force against (for example) a locked door to a room that an authorised officer requires access to in order to comply with the request from the Secretary and the relevant entity is refusing to provide the necessary assistance. Read together with section 35BB, the use of force against property is intended to be used as a last resort, when strictly necessary, to implement the request. The significance of this, further justifies the need for the Prime Minister and Defence Minister to agree to the giving of a relevant Ministerial authorisation.

206. Nevertheless, section 35BE clarifies that the use of force against a person by a constable or a staff member of the authorised agency is not authorised under this regime. This however would not exclude a police officer using force to arrest a person, under powers derived from other Commonwealth laws, who is obstructing a Commonwealth official in the performance of their functions (an offence under section 149.1 of the Criminal Code).

Section 35BD Removal and return of computers etc.

207. New section 35BD of the SOCI Act sets out obligations on approved staff members of the authorised agency to remove and return computers. This is an importance provision in ensuring that the asset, and its components, are reinstated as soon as practicable and to the extent possible to minimise any unnecessary impact of the exercise of the powers.

Subsection 35BD(1)-(2)—Removal of computers etc.

208. The connection of computers or other devices may be necessary to comply with a request under section 35AX, such as those of the authorised agency, may be required to, for example, undertake an analysis of a system onsite using specialised software. Subsection (1) provides that, if the authorised agency adds or connects a computer or device to a computer network and, whilst the relevant section 35AX request is in force, a staff member of the authorised agency forms a reasonable belief that the computer or device is no longer required to comply with the request, then the authorised agency must remove or disconnect the

computer or device as soon as practicable. This ensures that the intervention continues for no longer than is strictly necessary to comply with the request.

209. Under subsection (2), the obligation to remove a computer or device as soon as practicable also applies in circumstances where the request under section 35AX ceases to be in force—such as where the request expires or is revoked by the Secretary under section 35BA.

Subsection 35BD(3)-(4)—Return of computers etc.

210. The removal of computers may be necessary to comply with a request under section 35AX, for example, in instances where the authorised agency requires the use of specialised equipment located off-site to undertake the requested analysis.

211. Subsection (3) provides that, if the authorised agency removes a computer or device and, whilst the relevant section 35AX request is in force, an approved staff member of the authorised agency forms a reasonable belief that the removal of the computer or device is no longer required to comply with the request, then the authorised agency must return the computer or device as soon as practicable. This ensures that the intervention continues for no longer than is strictly necessary to comply with the request.

212. Under subsection (4), the obligation to return a computer or device as soon as practicable also applies in circumstances where the request under section 35AX ceases to be in force—such as where the request expires or is revoked by the Secretary under section 35BA.

Section 35BE Use of form against an individual not authorised

213. New section 35BE outlines that nothing in Division 5 of Part 3A of the SOCI Act (in particular, but not limited to, section 35BC) authorises the use of force against an individual. This is an important clarifying provision to ensure that, despite the importance of the powers being exercised, the use of force against a person is not justified under this regime noting its focus is on resolving cyber security incidents. This does not limit the use of force against a person being used concurrently when authorised under another law of the Commonwealth.

Section 35BF Liability

214. New section 35BF of the SOCI Act provides that the chief executive of the authorised agency, an approved staff member of the authorised agency or a constable is not liable to an action or other proceeding (whether civil or criminal) for, or in relation to, an act or matter done or omitted to be done in the exercise of any power or authority conferred by Division 5 of Part 3A of the SOCI Act. That is, the agency, staff member or constable is immune from liability when acting with lawful authority, providing the requisite legal certainty for those officers to take the necessary steps to comply with the request and protect Australia's national interests.

215. This immunity provision is reasonable and proportionate noting the various safeguards in place to ensure that actions or things lawfully authorised to be done or omitted under the Division are strictly limited, justified in the context of the cyber security incident and its impacts, and otherwise appropriate in all the circumstances. Further the oversight arrangements in place under the respective regimes of the Inspector-

General of Intelligence and Security and Commonwealth Ombudsman will ensure any misuse of the powers is identified and addressed.

Section 35BG Evidentiary certificates

216. New section 35BG of the SOCI Act provides that the Inspector-General of Intelligence and Security may issue a written certificate setting out any facts relevant the question of whether anything done, or omitted to be done, by the authorised agency, or an approved staff member of the authorised agency, was done, or omitted to be done, in the exercise of any power or authority conferred by the Division. For example, the evidentiary certificate may go to whether the execution of a computer program in a particular manner was in compliance with a request from the Secretary, and therefore authorised to occur. This is likely to rely on a strong understanding of technical matters which the Inspector-General of Intelligence and Security is well versed.

217. Subsection (2) provides that a certificate under subsection (1) is admissible in evidence in any proceedings as prima facie evidence of the matters stated in the certificate.

218. Evidentiary certificates are intended to streamline the court process by reducing the need to contact numerous officers and experts to give evidence. Evidentiary certificates also assist with maintaining the confidentiality of the sensitive methodologies and capability of the authorised agency. In this circumstance the matters it can be expected to cover are technical and non-controversial matters.

Section 35BH Chief executive of the authorised agency to report to the Defence Minister and the Minister

219. New section 35BH of the SOCI Act sets out requirements for the chief executive of the authorised agency to report on any activities undertaken under Division 5 of Part 3A of the SOCI Act.

220. This section establishes a requirement for the authorised agency to prepare a post-activity report that is to be provided to the Defence Minister, as Minister responsible for the authorised agency, and the Minister for Home Affairs, as the Minister responsible for the security of critical infrastructure and who authorised the request. This obligation is to ensure the relevant Ministers have visibility of the actions that were taken and how they contributed to an effective response. This will assist the Government in monitoring the use of these powers, but also support future decision making in similar circumstances.

221. Subsection (1) applies where the Secretary has given a request to the chief executive under section 35AX, that was authorised by a Ministerial authorisation given under paragraphs 35AB(2)(e) or (f), and the authorised agency does one or more acts or things in compliance with the request—as specified in the Ministerial authorisation and listed in section 35AC.

222. If subsection (1) applies, the chief executive of the authorised agency must:

- prepare a written report that sets out details of the acts or things done and explains the extent to which doing those acts or things has amounted to an effective response to the cyber security incident concerned (paragraph (c)), and

- give a copy of the report to the Defence Minister and Minister for Home Affairs (paragraphs (d) and (e)).

223. Subsection (2) requires the chief executive of the authorised agency to comply with the obligations under subsection (1) as soon as practicable after the end of the period specified in the section 35AX request and, in any event, within 3 months after the end of that period. This means that the report described in paragraph (1)(c) must be prepared and given to the respective Ministers no later than 3 months after the end of the period specified by the Secretary in the section 35AX request.

Section 35BJ Approved staff members of the authorised agency

224. Subsection (1) provides that the chief executive of the authorised agency may, in writing, declare that a specified staff member of the authorised agency is an approved staff member of the authorised agency for the purposes of this Act. Subsection (2) provides that subsection (1) is not a legislative instrument.

35BK Reports to the Parliamentary Joint Committee on Intelligence and Security

225. New section 35BK provides for reports to be made to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) about use made of the powers in Part 3A of the Act.

226. Subsection 35BK(1) requires the Secretary to give the PJCIS a written report about a cyber security incident in relation to which directions or requests in relation to government assistance measures are given or made under new sections 35AK, 35AQ or 35AX . Subsection 35BK(2) provides that the report must describe each of the directions or requests made in relation to the incident.

227. The Secretary is not required to make a separate written report to the PJCIS in relation to each direction or request, but is required to describe each direction or request in a report relating to each incident.

228. However, the Secretary may make more than one report to the PJCIS about a cyber security incident if, for example, the incident is ongoing. This could mean, for example, that an earlier report to the PJCIS describes earlier uses of the Part 3A powers in relation to the incident, while a later report describes later uses of the Part 3A powers in relation to the same incident.