
Cat Barker
Foreign Affairs, Defence and Security Section

Contents

The Bills Digest at a glance ................................................... 4
Purpose of the Bills .............................................................. 5
Structure of the Bills ............................................................ 5
Commencement details ....................................................... 5
Background ......................................................................... 6
Critical infrastructure............................................................... 6
Policy rationale and context for the Bill ......................... 6
Sectors and number of assets covered ............................... 8
Consultations on the measures in the Bill ....................... 8
Committee consideration .................................................... 9
Parliamentary Joint Committee on Intelligence and Security................................................................. 9
Senate Standing Committee for the Scrutiny of Bills .... 10
Policy position of non-government parties/independents... 10
Position of major interest groups ........................................ 10
Submissions in response to the February 2017 discussion paper ................................................................. 10
State and territory government positions on the Exposure Draft and final Bill ................................... 11
Sectors covered................................................................... 12
Affected sectors’ positions on the Exposure Draft and final Bill ......................................................... 12
Sectors covered................................................................... 12
Regulatory burden and costs ............................................. 13

Date introduced:  7 December 2017

House:  Senate

Portfolio:  Home Affairs (Attorney-General when introduced)

Commencement:  Refer to page 5 of this Digest for details.


When Bills have been passed and have received Royal Assent, they become Acts, which can be found at the Federal Register of Legislation website.

All hyperlinks in this Bills Digest are correct as at March 2018.
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other issues</td>
<td>13</td>
</tr>
<tr>
<td>Other stakeholders positions on the Exposure Draft and final Bill</td>
<td>14</td>
</tr>
<tr>
<td>Sectors covered</td>
<td>14</td>
</tr>
<tr>
<td>Other issues</td>
<td>14</td>
</tr>
<tr>
<td>Financial implications</td>
<td>14</td>
</tr>
<tr>
<td>Statement of Compatibility with Human Rights</td>
<td>14</td>
</tr>
<tr>
<td>Parliamentary Joint Committee on Human Rights</td>
<td>14</td>
</tr>
<tr>
<td>SCI Bill: key issues and provisions</td>
<td>15</td>
</tr>
<tr>
<td>Object</td>
<td>15</td>
</tr>
<tr>
<td>Constitutional provisions and application of the Act</td>
<td>15</td>
</tr>
<tr>
<td>Issue: constitutionality and impact on states</td>
<td>15</td>
</tr>
<tr>
<td>Critical infrastructure assets</td>
<td>15</td>
</tr>
<tr>
<td>Issue: lack of certainty about what constitutes a critical infrastructure asset</td>
<td>17</td>
</tr>
<tr>
<td>Prescription of assets (public)</td>
<td>17</td>
</tr>
<tr>
<td>Issue: prescription of additional classes of assets</td>
<td>17</td>
</tr>
<tr>
<td>Declaration of assets (not public)</td>
<td>18</td>
</tr>
<tr>
<td>Issue: lack of consultation requirements for declared assets</td>
<td>18</td>
</tr>
<tr>
<td>Issue: whether the Bill should apply to additional sectors</td>
<td>18</td>
</tr>
<tr>
<td>Reporting entities and operators</td>
<td>19</td>
</tr>
<tr>
<td>Issue: definition of direct interest holder</td>
<td>19</td>
</tr>
<tr>
<td>Register of Critical Infrastructure Assets (Part 2)</td>
<td>20</td>
</tr>
<tr>
<td>Establishment of the Register</td>
<td>20</td>
</tr>
<tr>
<td>Information that must be provided by reporting entities initially</td>
<td>20</td>
</tr>
<tr>
<td>Ongoing obligations to provide information</td>
<td>21</td>
</tr>
<tr>
<td>Civil penalties</td>
<td>21</td>
</tr>
<tr>
<td>Exceptions and exemptions to obligations to provide information</td>
<td>21</td>
</tr>
<tr>
<td>Notification of change of reporting entities for assets declared under clause 51</td>
<td>22</td>
</tr>
<tr>
<td>Power for the Minister to issue directions (Part 3)</td>
<td>22</td>
</tr>
<tr>
<td>When a direction may be issued</td>
<td>22</td>
</tr>
<tr>
<td>Consultation requirements</td>
<td>23</td>
</tr>
<tr>
<td>Review of decisions</td>
<td>23</td>
</tr>
<tr>
<td>Issue: thresholds for issue of directions and matters to be considered beforehand</td>
<td>24</td>
</tr>
<tr>
<td>Issue: interaction of directions power with other laws</td>
<td>24</td>
</tr>
<tr>
<td>Compliance and civil penalty</td>
<td>24</td>
</tr>
<tr>
<td>Gathering and using information (Part 4)</td>
<td>24</td>
</tr>
<tr>
<td>Secretary’s powers to compel information and documents</td>
<td>24</td>
</tr>
</tbody>
</table>

Warning: All viewers of this digest are advised to visit the disclaimer appearing at the end of this document. The disclaimer sets out the status and purpose of the digest.
Issue: scope of notice and time for compliance................. 25
Authorised use and disclosure of protected information................................................................. 25
Issue: Secretary’s powers to share protected information............................................................. 26
Unauthorised use and disclosure of protected information............................................................. 26

SCI Bill: other provisions ................................................. 27
Enforcement (Part 5) ........................................................................ 27
Administrative provisions (Part 7) ................................................................. 27
Application to certain entities................................................................. 27
Secretary’s powers ........................................................................ 27
Annual reports............................................................................. 27
Rules.......................................................................................... 27

Consequential and Transitional Provisions Bill............ 28
Consequential amendments................................................................. 28
Other amendments........................................................................ 28
The Bills Digest at a glance

Purpose and background

The Security of Critical Infrastructure Bill 2017 (the SCI Bill) will:

• establish a Register of Critical Infrastructure Assets that will include information about who owns and operates those assets and which must not be made public and
• allow the Minister to give a direction to a reporting entity or an operator of a critical infrastructure asset to do, or refrain from doing, a specified act or thing within a certain timeframe. The power may be used if the Minister is satisfied that there is a risk that is prejudicial to security that cannot otherwise be mitigated.

These measures will initially apply to critical infrastructure assets in the electricity, gas, water and ports sectors.

The SCI Bill is intended to strengthen the Government’s capacity to manage the national security risks of espionage, sabotage and coercion that arise from foreign involvement in Australia’s critical infrastructure. Its introduction follows on from several other developments related to improving the resilience of Australia’s critical infrastructure and increased attention on the security risks associated with foreign investment in critical infrastructure. These include reforms designed to better manage national security risks to Australia’s telecommunications networks and facilities and tighter restrictions on foreign investment in critical infrastructure.

Committee consideration

The Parliamentary Joint Committee on Intelligence and Security tabled its report on the SCI Bill on 15 March 2018. The Committee recommended relatively minor amendments to the SCI Bill, but also made several non-legislative recommendations.


The Senate Standing Committee for the Scrutiny of Bills raised two issues in relation to the SCI Bill—the ability for the Minister to make rules that would amend the operation of primary legislation (by providing that certain provisions do not apply to certain entities); and the inclusion of offence-specific exceptions to the proposed offence for unauthorised use or disclosure of protected information, for which defendants would bear an evidential burden.

Stakeholder reaction

Stakeholders were supportive of the Bill’s objectives, but most had some concerns about the application and operation of the proposed register and ministerial direction power.

Issues raised by state and territory governments included the potential for the measures in the SCI Bill to be exercised in way that impairs the capacity of the states to exercise their constitutional powers and the related issue of the application of the measures to critical infrastructure assets owned and/or operated by state and territory governments; consultation requirements; potential costs to states and territories associated with compliance with directions issued by the Minister; a lack of clarity as to what constitutes a critical infrastructure asset and particular types of asset; how information included in the register will be secured and protected and information sharing arrangements.

Issues raised by stakeholders from affected sectors included the need to minimise regulatory burden; how costs associated with complying with a ministerial direction could be recovered; a lack of clarity as to what constitutes a critical infrastructure asset and particular types of asset; how information included in the register will be secured and protected; the breadth of the Secretary’s powers to disclose protected information and the potential for ministerial directions to require actions that would conflict with requirements under other laws.

Several stakeholders considered that the measures should be extended to additional sectors, such as data centres, health and medical facilities, the finance and banking sector, airports and the transport sector. The Bill will provide a mechanism for additional assets and classes of assets to be included in future.
Purpose of the Bills
The purpose of the Security of Critical Infrastructure Bill 2017 (the SCI Bill) is to:

• establish a Register of Critical Infrastructure Assets that will include information about who owns and operates those assets and which must not be made public and
• allow the Minister to give a direction to a reporting entity or an operator of a critical infrastructure asset to do, or refrain from doing, a specified act or thing within a certain timeframe. The power may be used if the Minister is satisfied that there is a risk that is prejudicial to security that cannot otherwise be mitigated.

The Department of Home Affairs will administer the Act; however, it is unclear which Minister in that portfolio will issue directions. The power would appear likely to rest with either the Minister for Home Affairs or the Minister for Law Enforcement and Cybersecurity.

The purposes of the Security of Critical Infrastructure (Consequential and Transitional Provisions) Bill 2017 (Consequential and Transitional Provisions Bill) are to make consequential amendments to the Australian Security Intelligence Organisation Act 1979 (ASIO Act) and the Foreign Acquisitions and Takeovers Act 1975 (FATA), and to amend the FATA to allow disclosure of protected information within the meaning of the FATA to be shared with the Minister for Defence and the Secretary of the Department of Defence.

Structure of the Bills
The SCI Bill contains seven Parts:

• Part 1 contains definitions of key terms used throughout the Bill, constitutional provisions and provisions about the application of the Bill.
• Part 2 will establish the register and related requirements for entities to provide information.
• Part 3 will establish the ministerial directions power.
• Part 4 will provide information gathering powers and set out how information obtained under the Bill may be used and disclosed. It also includes an offence for unauthorised use or disclosure.
• Part 5 will provide that civil penalty provisions in the Bill are enforceable under certain parts of the Regulatory Powers (Standard Provisions) Act 2014 (Regulatory Powers Act).
• Part 6 will allow the Minister to privately declare assets to be critical infrastructure assets if satisfied of certain matters.
• Part 7 will set out how the Bill applies to certain entities, provide for matters relevant to the Secretary’s powers, require annual reports on the measures in the Bill, and allow the Minister to make rules by legislative instrument.

The Consequential and Transitional Provisions Bill contains two Schedules:

• Schedule 1 contains amendments to the ASIO Act and the FATA that are consequential to the SCI Bill.
• Schedule 2 will make an unrelated amendment to the FATA to allow disclosure of protected information within the meaning of the FATA to be shared with the Minister for Defence and the Secretary of the Department of Defence.

Commencement details
The SCI Bill will commence on proclamation or three months after Royal Assent, whichever occurs first.

Clauses 1–3 of the Consequential and Transitional Provisions Bill will commence on Royal Assent. Schedule 1 will commence immediately after the commencement of section 32 of the Security of Critical Infrastructure Act. Schedule 2 will commence the day after Royal Assent.

1. Department of Home Affairs, Submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS), Inquiry into the Security of Critical Infrastructure Bill 2017, n.d., pp. 3–4. There are several Ministers within the Home Affairs portfolio (Minister for Home Affairs, Minister for Immigration and Border Protection, Minister for Citizenship and Multicultural Affairs, Minister for Law Enforcement and Cybersecurity and Assistant Minister for Home Affairs).
Background

Critical infrastructure

The Australian and state and territory governments define critical infrastructure as:

... those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation or affect Australia’s ability to conduct national defence and ensure national security.2

It includes, for example, infrastructure associated with delivering essential services such as food, water, power and healthcare (though the measures in the Bill will not, at least initially, apply to all types of critical infrastructure).

Policy rationale and context for the Bill

The Government has stated that the SCI Bill aims to strengthen its capacity to manage the national security risks of espionage, sabotage and coercion that arise from foreign involvement in Australia’s critical infrastructure.3 It described those risks as follows:

- **Espionage**: Certain critical infrastructure sectors may present opportunities for the collection of information which is not publicly available. Foreign intelligence services will target commercial as well as government-related organisations for this data. For example, a telecommunications operator or contractor could monitor customers’ voice or data traffic to gather information on behalf of a foreign intelligence service.

- **Sabotage**: A hostile foreign actor could use access gained through investment or commercial involvement to conduct a deliberate disruption to supply for strategic or economic gain. For example, the deliberate interruption or destruction of operations at a port could result in economic and reputational damage for the Government.

- **Coercion**: In extreme cases, a foreign actor could use access to critical infrastructure to apply coercive power against the Australian Government to influence decision-making or policy.[emphasis added]4

Most of Australia’s critical infrastructure is privately owned and operated, or run on a commercial basis by government, and responsibility for continued operations and service provision is shared between Australian governments and the private sector.5 While the Government has recognised that owners and operators of Australia’s critical infrastructure ‘understand and manage many of the risks to continuity of their operations as a core part of their business’, it wants to ensure that it is in a position to ‘develop a comprehensive picture of national security risks from foreign involvement in critical infrastructure, and apply appropriate mitigations where necessary’.6

Introduction of the SCI Bill follows on from several other developments related to improving the resilience of Australia’s critical infrastructure and increased attention on the security risks associated with foreign investment in critical infrastructure:

- In May 2015 the Government released a new Critical Infrastructure Resilience Strategy, the objectives of which are that critical infrastructure owners and operators are ‘effective in managing foreseeable risks to the

---

2. Australian Government, Critical infrastructure resilience strategy: policy statement, Commonwealth of Australia, 2015, p. 3. ‘Significantly’ means ‘an event or incident that puts at risk public safety and confidence, threatens our economic security, harms Australia’s international competitiveness, or impedes the continuity of government and its services’


6. Ibid., p. 4; Explanatory Memorandum, SCI Bill, p. 6.
continuity of their operations through a mature risk-based approach’ and ‘effective in managing unforeseen
risks to the continuity of their operations through an organisational resilience approach’ (emphasis added). 7

• In March 2016 the Government tightened foreign investment rules so that the Foreign Investment Review
Board now assesses the sale of critical infrastructure by state and territory governments to private foreign
investors. 8 The change followed the Northern Territory (NT) Government’s granting of a long-term lease for
the Port of Darwin to Chinese company Landbridge in October 2015. 9

• In November 2016 the Government introduced reforms ‘to better manage national security risks of
espionage, sabotage and foreign interference to Australia’s telecommunications networks and facilities’. 10

The legislation was passed by the Parliament in 2017, and the Telecommunications and Other Legislation
Amendment Act 2017 will commence in September 2018. It will introduce an obligation on carriers, carriage
service providers and carriage service intermediaries to do their best to protect networks and facilities from
unauthorised access and interference; an obligation on carriers and some carriage service providers to notify
the Government of planned changes to their networks and services that might compromise their ability to
comply with the security obligation; and a power for the Minister to direct a carrier, carriage service provider
or carriage service intermediary to take action that is reasonably necessary to protect a network or facility
from a national security risk.11 The proposed ministerial directions power in the SCI Bill is modelled on this
one.

• David Irvine, former head of the Australian Security Intelligence Organisation (ASIO) and the Australian Secret
Intelligence Service, was appointed to the Foreign Investment Review Board in December 2015, and
appointed as its Chair in April 2017. 12

• The Government established the Critical Infrastructure Centre in January 2017:13

The Centre focuses on the potential for malicious actors to gain access and control to Australia’s critical
infrastructure, through ownership, offshoring, outsourcing and supply chain arrangements. The Centre collaborates
with owners and operators and state and territory regulators to identify risks and develop and implement asset-
specific mitigation strategies and sector-wide best practice guidelines.14

The SCI Bill was introduced on the same day as the Government’s espionage, foreign interference and foreign
influence reforms.15 The Department of Home Affairs noted that the National Security Legislation Amendment
(Espionage and Foreign Interference) Bill 2017:

... complements the work of the Centre and the Bill, by strengthening existing espionage offences and introducing
comprehensive new sabotage offences, which will enable the Government to prosecute malicious actors, including
those that use critical infrastructure to engage in espionage and sabotage activities.16

Finally, in February 2018, the Government announced that ‘all future applications for the sale of electricity
transmission and distribution assets, and some generation assets, will attract ownership restrictions or

7. G Brandis (Attorney-General), Address to the Critical Infrastructure Resilience Conference, Sydney, media release, 21 May 2015; Australian
Government, Critical infrastructure resilience strategy: policy statement, op. cit., pp. 7–8. The Strategy comprises a policy statement and a
8. S Morrison (Treasurer), Critical asset sales to fall within foreign review net, media release, 18 March 2016; Foreign Acquisitions and Takeovers
Amendment (Government Infrastructure) Regulation 2016.
Security experts were divided on whether the lease should have been granted; see for example: P Barnes et al, Chinese investment in the Port
of Darwin: a strategic risk for Australia?, Australian Strategic Policy Institute, December 2015.
10. Revised Explanatory Memorandum, Telecommunications and Other Legislation Amendment Bill 2017, p. 2. See also G Brandis (Attorney-
General) and M Fifield (Minister for Communications), Protecting vital telecommunications networks, media release, 9 November 2016.
11. Attorney-General’s Department (AGD), Telecommunications sector security reforms, AGD website.
12. S Morrison (Treasurer), Security and business expertise added to Foreign Investment Review Board, media release, 4 December 2015;
S Morrison (Treasurer), FIRB chair appointment, media release, 8 April 2017.
15. These reforms comprise the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017, Foreign Influence
Transparency Scheme Bill 2017, Foreign Influence Transparency Scheme (Charges Imposition) Bill 2017 and the Electoral Legislation
Amendment (Electoral Funding and Disclosure Reform) Bill 2017.
conditions for foreign buyers’ to allow it to actively manage the level of ownership and control from investors in a single asset or within a sector.\textsuperscript{17}

\textbf{Sectors and number of assets covered}

The Government determined the highest-risk sectors on the basis of two factors: risks of espionage, sabotage and coercion by foreign actors, and whether existing regulatory regimes for different sectors would support federal government direction.\textsuperscript{18}

The Government considers that risks of espionage, sabotage and coercion are highest in relation to the telecommunications, electricity, water and ports sectors.\textsuperscript{19} The two measures in the Bill—the register and the ministerial directions power—will initially apply to critical infrastructure assets in the electricity, water, ports and gas sectors (the last of these having been added following consultations). As noted above, an equivalent directions power was established in relation to the telecommunications sector, along with security and notification obligations, in 2017. The SCI Bill will enable other sectors to be added at a later date.

The Government expects the SCI Bill to apply to approximately 140 assets across the electricity, water, ports and gas sectors.\textsuperscript{20}

\textbf{Consultations on the measures in the Bill}

The Government conducted two rounds of public consultation on the measures included in the Bill in 2017.

On 21 February 2017 the Government released a discussion paper seeking stakeholder views on potential measures to strengthen the national security of Australia’s critical infrastructure, including the two measures now included in the Bill.\textsuperscript{21}

An Exposure Draft of the Bill was then released for comment on 10 October 2017.\textsuperscript{22} The main differences between the Exposure Draft and the SCI Bill are that the latter:

- will apply to critical assets in the gas sector as well as those in the electricity, water and ports sectors (\textit{clauses 9} and \textit{12})
- includes definitions of \textit{First Minister}, \textit{international relations} and \textit{national security} and amended definitions relevant to \textit{critical water assets} (\textit{clause 5})
- will provide for civil penalties of up to 50 penalty units (instead of 25) for reporting entities failing to notify the Secretary of notifiable events (\textit{clause 24})
- includes an exception to obligations to provide the Secretary with certain information where a person is not able to obtain the information despite the person’s best endeavours (\textit{clause 25})
- will require the Minister to be ‘satisfied that no existing regulatory system of the Commonwealth, a State or a Territory could instead be used to eliminate or reduce the risk’ concerned before giving a direction (whether existing systems could be used was previously only a matter to which consideration was to be given) (\textit{clause 32})
- includes more stringent requirements for consultation with the government of the relevant state or territory before the Minister gives a direction (\textit{under clause 32}) to a reporting entity for or operator of a critical infrastructure asset (\textit{clause 33})
- will allow \textit{protected information} to be disclosed to a federal minister who has responsibility for law enforcement (\textit{clause 42})

\textsuperscript{17} S Morrison (Treasurer) and P Dutton (Minister for Home Affairs), \textit{New conditions on the sale of Australian electricity assets to foreign investors}, media release, 1 February 2018.

\textsuperscript{18} Department of Home Affairs, Submission to the PJCIS, op. cit., pp. 5–6.


\textsuperscript{20} Explanatory Memorandum, SCI Bill, p. 7.

\textsuperscript{21} CIC, \textit{Strengthening the national security of Australia’s critical infrastructure: a discussion paper}, op. cit., pp. 9–12; AGD, ‘\textit{Strengthening the national security of Australia’s critical infrastructure}’, AGD website.

\textsuperscript{22} G Brandis (Attorney-General), \textit{New measures to safeguard Australia’s critical infrastructure}, media release, 10 October 2017; \textit{Security of Critical Infrastructure Bill 2017: exposure draft}.
• will require the Minister to notify the First Minister of the state or territory in which any asset declared under clause 51 is located of the declaration (but only after the event)

• includes an obligation for reporting entities for assets declared under clause 51 to notify the Secretary if they cease to be a reporting entity or become aware of another reporting entity (clause 52)

• will require the Secretary to notify a reporting entity if he or she becomes aware that the asset has ceased to be a critical infrastructure asset (clause 58).

Stakeholder views are summarised below under ‘Position of major interest groups’.

Committee consideration

Parliamentary Joint Committee on Intelligence and Security

The Parliamentary Joint Committee on Intelligence and Security (PJCIS) tabled its report on the SCI Bill on 15 March 2018. The PJCIS recommended that the SCI Bill should be amended to:

• more appropriately define direct interest holder (in relation to a critical infrastructure asset) in order to capture the intended range of ownership arrangements, and clarify that:
  – moneylenders are not direct interest holders where they hold an interest through a financing arrangement and
  – intermediate and ultimate holding entities are not direct interest holders (Recommendation 4)

• require the Minister to provide notice of an adverse security assessment made for the purposes of the proposed ministerial directions power in Part 3 of the SCI Bill to the entity to which it relates (Recommendation 8) and

• require the Committee to review the operation, effectiveness and implications of the proposed reforms within three years of the Bill receiving Royal Assent (Recommendation 9). 23

The PJCIS recommended that the Explanatory Memorandum to the SCI Bill be amended to:

• clarify the scope of the definition of direct interest holder (further to amendments to the SCI Bill) (Recommendation 4)

• include the factors to which the Secretary must have regard when deciding whether to disclose protected information under clauses 42 and 43 (Recommendation 6) and

• clarify that the SCI Bill, particularly clause 39, does not affect the operation of existing privacy obligations (Recommendation 7). 24

It also recommended that:

• the Government review and develop measures to ensure that Australia has a continuous supply of fuel to meet its national security priorities and brief the Committee on the outcomes of the review (Recommendation 1)

• the Department of Home Affairs examine the viability of developing a common data entry portal for use across Commonwealth, state and territory databases that require information from the same entities (Recommendation 2)

• the Department of Home Affairs develop guidelines for entities subject to the SCI Bill (Recommendation 3) and

• the guidelines include information on the high-level criteria by which the Department of Home Affairs will assess risk and the process and engagement that entities should reasonably expect from the Department as part of a risk assessment (Recommendation 5). 25


24. Ibid., pp. xii–xiii. See further pp. 28–32 (direct interest holders), p. 40 (disclosure of protected information) and pp. 35–9, 41 (privacy).

25. Ibid., pp. xi–xii. See further pp. 18–22 (fuel security), pp. 24–31 (information reported to Commonwealth, state and territory governments) p. 31 (guidelines) and pp. 33–5, 39–40 (risk assessments).
The PJCIS recommended that subject to the above recommendations being accepted, the SCI Bill should be passed.²⁶

**Senate Standing Committee for the Scrutiny of Bills**

The Senate Standing Committee for the Scrutiny of Bills (Scrutiny of Bills Committee) raised two issues in relation to the SCI Bill.

**Division 3 of Part 2** of the Bill will impose obligations on reporting entities (clauses 23 and 24) and entities that will be reporting entities at the end of the six month grace period (clause 23) to provide certain information to the Secretary. **Clause 27** will allow the rules (which the Minister will be able to make under clause 61) to provide that Division 3 of Part 2, or specific provisions within it, do not apply in relation to any entity, specified classes of entities or specified entities. The Scrutiny of Bills Committee objected to clause 27 on the basis that it “effectively allows the rules to amend the operation of proposed Division 3 (that is, to amend the primary legislation)”.²⁷ It considered that the Explanatory Memorandum did not provide sufficient justification for this, and sought the Minister’s more detailed justification for the provision and advice as to whether it would be appropriate to amend the Bill to insert guidance about the making of rules for the purposes of clause 27.²⁸

**Clause 45** will establish an offence for unauthorised disclosure of protected information. **Clause 46** will provide for three specific exceptions to the offence. An entity wishing to rely on any of these exceptions in proceedings for an offence against clause 45 will bear an evidential burden in relation to the matter (which would require adducing or pointing to evidence that suggests a reasonable possibility that the matter exists).²⁹ The Scrutiny of Bills Committee recognised that the defendant will bear only an evidential rather than a legal burden, but nonetheless stated that it expected any reversal of the burden of proof to be justified.³⁰ As the Explanatory Memorandum does not provide that justification, the Committee requested the Minister’s advice as to why offence-specific exceptions have been proposed in this instance.³¹

**Policy position of non-government parties/independents**

The Shadow Assistant Minister for Cyber Security and Defence, Gai Brodtmann, wrote to the Attorney-General about the Exposure Draft Bill and recommended that the Bill should apply to critical infrastructure assets in the same sectors that participate in the Trusted Information Sharing Network (TISN).³² The TISN is the primary national mechanism for government-business engagement and information sharing on critical infrastructure resilience, and includes eight sector groups—banking and finance, communications, energy, food and grocery, health, transport, water services and Commonwealth Government.³³ Ms Brodtmann also questioned why the Bill would apply to sea ports but not airports and suggested that consideration be given to expanding both the TISN and the Bill to include additional sectors, such as emergency services, information technology, chemicals and manufacturing.³⁴

At the time of publication of this Bills Digest, the Australian Labor Party did not appear to have commented publicly on the final Bill, and there was no public indication of the policy position of any other non-government parties and independents on the SCI Bill.

**Position of major interest groups**

**Submissions in response to the February 2017 discussion paper**

The Attorney-General’s Department (AGD) has published 41 of the submissions it received in response to the February 2017 discussion paper that included proposals for a register and directions power.³⁵ Many of the

---

²⁶. Ibid., p. xiii.
²⁷. Senate Standing Committee for the Scrutiny of Bills (Scrutiny of Bills Committee), Scrutiny digest, 1, 2018, The Senate, 7 February 2018, p. 97.
²⁸. Ibid., pp. 97–8.
³¹. Ibid., p. 99.
³⁵. AGD, ‘Strengthening the national security of Australia’s critical infrastructure’, op. cit. Submissions provided on a confidential basis were not published.
submissions did not state whether or not the submitter generally supported the measures, but rather focused on potential issues and questions they had about them. Broadly, submissions from state and territory governments (Australian Capital Territory (ACT), New South Wales (NSW), NT, Queensland and Tasmania) sought further detail and consultation on the proposed measures, including how they would interact with state responsibilities; raised concerns relating to potential duplication and associated regulatory burden; and queried how costs relating to compliance with ministerial directions would be met. Themes that emerged from industry submissions included concerns about regulatory burden and costs relating to compliance with ministerial directions, concerns and questions about how the proposed measures would interact with existing regulatory frameworks (particularly at state and territory level) and the importance of ensuring the security of information included in the proposed register.37

State and territory government positions on the Exposure Draft and final Bill38

The South Australian (SA), NSW, NT and ACT Governments made public submissions to AGD on the Exposure Draft Bill. These governments were supportive of the Bill’s objectives, but raised some concerns with aspects of the Exposure Draft, and all except the ACT Government considered that the timeframe for submissions was too short.39 Some of the main concerns related to:

- the constitutionality of the Bill, particularly the potential for the measures it contains to be exercised in a way that impairs the capacity of the states to exercise their constitutional powers, in violation of the Melbourne Corporation principle.40
- the application of the measures in the Bill to critical infrastructure assets owned and/or operated by state and territory governments41
- the need to strengthen requirements relating to consultation with state and territory governments prior to the prescription or declaration of additional critical infrastructure assets (addressed to some extent in the Bill)42
- potential costs to states and territories associated with compliance with directions issued by the Minister, either directly, or indirectly through possible claims against a state or territory government43


37. Submissions from the following organisations and bodies were published: Airservices Australia; Arup; Ausgrid; N. Australian Maritime Officers Union; Australian Pipelines and Gas Association; BAE Systems Applied Intelligence; Centre for Disaster Management and Public Safety (University of Melbourne); CitiPower and Powercor Australia; CSIRO; Curtis Incorporated; Energy Networks Australia; Geoscience Australia; Hasting; Independent Pricing and Regulatory Tribunal (NSW); Infrastructure Partnerships Australia; Law Council of Australia; Local Government Association of Queensland; Office of the Australian Information Commissioner; Ports Australia; Queensland Water Directorate; Rail Industry Safety and Standards Board; Risk Frontiers; SGSP (Australia) Assets; Singapore Power Group; South Australia Energy and Technical Regulation; Symantec; Thales Australia and New Zealand; TransGrid; Vodafone Hutchinson Australia and Water Services Association of Australia. Several individuals also made submissions.

38. While this section incorporates information from submissions made in relation to the Exposure Draft, it focuses mainly on issues not already addressed through amendments to the Bill since the release of the Exposure Draft.


40. SA Government, Submission to AGD, op. cit., p. 1; NSW Government, Submission to AGD, Exposure Draft, op. cit., pp. 1–2; The Melbourne Corporation principle was established in Melbourne v Commonwealth [1947] HCA 26, 13 August 1947. The High Court has characterised the principle as being concerned with ‘whether impugned legislation is directed at States, imposing some special disability or burden on the exercise of powers and fulfilment of functions of the States which curtails their capacity to function as governments’: Fortescue Metals Group Limited v The Commonwealth [2013] HCA 33, 7 August 2013, at [131].

41. NSW Government, Submission to AGD, Exposure Draft, op. cit., pp. 1–2; SA Government, Submission to AGD, op. cit., p. 1. The NSW Government submission refers to and supports a proposal by the Victorian Government to exclude state owned and operated assets from the Bill. The Victorian Government did not make a public submission.

42. NSW Government, Submission to AGD, Exposure Draft, op. cit., pp. 2–3, 6; SA Government, Submission to AGD, op. cit., p. 2; ACT Government, Submission to AGD, Exposure Draft, op. cit.
• a lack of clarity as to what constitutes a **critical infrastructure asset** and particular types of asset
• how information included in the register will be secured and protected and
• arrangements for sharing information provided by entities between the federal and state and territory governments, and with Commonwealth ministers for other purposes.

Only the SA Government made a submission to the PJCIS’s inquiry into the Bill. The SA Government welcomed changes made since the Exposure Draft, including strengthening requirements to consult with state and territory governments. However, it remained concerned about the ability for the Commonwealth to direct states and state instrumentalities, the lack of a requirement for the Minister to consult the relevant state before declaring assets to be critical infrastructure assets and potential costs. It also considered that amendments to the Bill and the Explanatory Memorandum since the Exposure Draft had introduced ambiguity, specifically a lack of clarity around the definitions of **critical infrastructure asset** and **direct interest holder**. In its supplementary submission to the PJCIS, the Department of Home Affairs stated that it would seek to amend the definition of **direct interest holder** to address concerns raised in submissions to the PJCIS’s inquiry into the SCI Bill.

**Sectors covered**

The NT Government suggested that the fuel sector should be considered for future inclusion in the measures introduced by the Bill.

**Affected sectors’ positions on the Exposure Draft and final Bill**

Similarly to state and territory governments, industry stakeholders generally supported the policy objectives of the Bill, but raised some concerns about aspects of the two measures, and about the degree to which they had been consulted, in submissions to the Exposure Draft consultations and the PJCIS’s inquiry.

**Sectors covered**

In its submission to the Exposure Draft consultations, ExxonMobil recommended against inclusion of critical gas or oil infrastructure, arguing that those sectors already have appropriate risk assessment and response systems in place. Energy Networks Australia stated that inclusion of the gas sector should be considered, but only after the risk assessment and reporting processes for the electricity, water and ports sectors were thoroughly tested and mature. In its submission to the PJCIS, Energy Networks Australia noted, but provided no comment on, the inclusion of the gas sector in the final Bill. The Australian Pipelines and Gas Association (APGA) suggested that consideration be given to removing gas transmission pipelines from the scope of the Bill or finding a less intrusive means of achieving the Bill’s objectives.

---

44. NSW Government, Submission to AGD, Exposure Draft, op. cit., p. 6; NT Government, Submission to AGD, Exposure Draft, op. cit., p. 6.
45. NSW Government, Submission to AGD, Exposure Draft, op. cit., p. 5; NT Government, Submission to AGD, Exposure Draft, op. cit., p. 5.
47. The NT Government provided a copy of its Exposure Draft submission to the PJCIS.
51. While this section incorporates information from submissions made in relation to the Exposure Draft, it focuses mainly on issues not already addressed through amendments to the Bill since the release of the Exposure Draft. If an organisation made a submission to AGD on the Exposure Draft and to the PJCIS on the Bill, the latter is primarily relied on here.
Regulatory burden and costs

Several stakeholders from the electricity, gas and water sectors considered that the Government had underestimated the costs of the measures to industry in the estimates released with the Exposure Draft.56 The estimates set out in the Regulatory Impact Statement are significantly higher than those included in the explanatory document that accompanied the Exposure Draft Bill.57 However, the Water Services Association of Australia (WSAA) maintained that concern in its submission to the PJCIS.58 APGA suggested that in place of the measures in the Bill, the Government could impose obligations relating to security of supply and assure itself that those obligations were being met by requiring annual statutory declarations and being able to order audits.59

In relation to the register, some stakeholders suggested that the regulatory burden could be minimised by the Government making use of information already provided to the federal and state and territory governments, and only requesting additional information where required to fill gaps.60

Some stakeholders noted that the costs associated with complying with ministerial directions could be significant, and suggested that consideration be given to how those costs would be able to be recovered, including whether the Commonwealth should be required to provide compensation.61 Energy Australia suggested that providing compensation for costs that cannot be passed on to customers would be likely to increase voluntary cooperation and reduce the need to use the directions power.62 APGA suggested that provision should be made for regulatory notices that recognise voluntary undertakings so that associated costs can be passed on in the same way as those associated with mandatory actions.63

Other issues

Other concerns raised by industry stakeholders included:

• a lack of clarity as to what constitutes a critical infrastructure asset and particular types of asset64
• how information included in the register will be secured and protected65
• the breadth of the Secretary’s powers to disclose protected information and66
• the potential for ministerial directions to require actions that would conflict with requirements under other laws.67

Further detail is provided where relevant in the ‘SCI Bill: key issues and provisions’ section of this Digest.


57. The Government estimated that the register will cost industry a total of $86,789 per year and that implementing ministerial directions will cost industry a total of $8.12 million per year (assuming the power is exercised once every three years): Regulatory Impact Statement (Appended to the Explanatory Memorandum to the SCI Bill), pp. 29–30 (for further detail, see pp. 10–27). For the earlier estimates, see CIC, Security of Critical Infrastructure Bill 2017: explanatory document, Australian Government, October 2017, pp. 43–5, 54–61.


59. APGA, Submission to the PICIS, op. cit., pp. 1–2.

60. Energy Australia, Submission to AGD, Exposure Draft of the Security of Critical Infrastructure Bill 2017, 10 November 2017, p. 2; ExxonMobil, Submission to AGD, op. cit.; ATCO Australia, Submission to AGD, op. cit., pp. 2–3; APGA, Submission to the PICIS, op. cit., pp. 3–6. The Regulatory Impact Statement indicates that this option was considered but was not the preferred option because it would ‘involve significant allocation of resources in the Australian Government and state governments’ and the resulting register ‘would still fall short’ of providing all of the necessary information: Regulatory Impact Statement, op. cit., pp. 5–6, 10.

61. ATCO Australia, Submission to AGD, op. cit., p. 2; WSAA, Submission to the PICIS, op. cit., pp. 5–6.


63. APGA, Submission to the PICIS, op. cit., p. 6.

64. Sydney Water, Submission to AGD, op. cit.; Hunter Water, Submission to AGD, op. cit.; ATCO Australia, Submission to AGD, op. cit., pp. 1–2; TasWater, Submission to AGD, Exposure Draft of the Security of Critical Infrastructure Bill 2017, 10 November 2017, pp. 1–2; WSAA, Submission to the PICIS, op. cit.; APGA, Submission to the PICIS, op. cit.


66. Energy Australia, Submission to AGD, op. cit., p. 2; Ausgrid, Submission to AGD, op. cit.; TasWater, Submission to AGD, op. cit., p. 2.

67. Energy Australia, Submission to AGD, op. cit., p. 2; TransGrid, Submission to AGD, op. cit., p. 3.
Other stakeholders positions on the Exposure Draft and final Bill

Sectors covered

In submissions to the PJCIS and earlier consultations, some stakeholders suggested the inclusion of additional sectors. Macquarie Telecom Group suggested that the Bill should apply to the same sectors that participate in the TISN. The National Archives of Australia recommended that data centres that hold information about critical infrastructure assets should themselves be treated as critical infrastructure assets. In a submission made in a personal capacity, Peter Jennings, head of the Australian Strategic Policy Institute, suggested that the Bill should also apply to data centre assets, medical facilities, blood and plasma storage, pharmaceutical supplies, the banking sector and airports. Doctors Against Forced Organ Harvesting also recommended the inclusion of healthcare and medical facilities. Arup suggested that the Bill should extend to the agriculture and food, emergency services, financial services, health, information technology and transport sectors.

Other issues

In its submission to the PJCIS, the Law Council of Australia (LCA) appears to generally support the Bill, but raised concerns about some specific aspects of the Bill, including the definition of direct interest holder and the threshold tests for exercise of the ministerial directions power.

The Inspector-General of Intelligence and Security (IGIS) did not comment on the substance of the Bill, but made a submission to the PJCIS in which she suggested an amendment to address a technical issue relating to notification requirements for adverse security assessments.

In its supplementary submission to the PJCIS, the Department of Home Affairs stated that it would seek to amend the SCI Bill to clarify the definition of direct interest holder and implement the change recommended by the IGIS.

Financial implications

The Explanatory Memorandum states that the SCI Bill has no financial impact, but notes that the Critical Infrastructure Centre, which will administer the register, has been allocated ongoing funding to understand and manage national security risks associated with foreign involvement in Australia’s critical infrastructure.

Statement of Compatibility with Human Rights

As required under Part 3 of the Human Rights (Parliamentary Scrutiny) Act 2011 (Cth), the Government has assessed the SCI Bill’s compatibility with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of that Act. The Government considers that the SCI Bill is compatible.

Parliamentary Joint Committee on Human Rights

The Parliamentary Joint Committee on Human Rights considers that neither of the Bills raises human rights concerns.
SCI Bill: key issues and provisions

Object
Clause 3 will provide that the object of the Act is to provide a framework for managing national security risks relating to critical infrastructure, including by:

(a) improving the transparency of the ownership and operational control of critical infrastructure in Australia in order to better understand those risks; and

(b) facilitating cooperation and collaboration between all levels of government, and regulators, owners and operators of critical infrastructure, in order to identify and manage those risks.

While the Bill will provide for significant ministerial powers, this clause indicates an intention for issues to be managed through cooperation and collaboration to the extent possible. The Parliament may wish to consider if the object is appropriately balanced in light of some of the concerns raised by state and territory governments and industry stakeholders.

Constitutional provisions and application of the Act
Clause 13 will set out the types of entities to which the Act will apply, framed around Commonwealth heads of power under the Constitution.
Clause 14 will provide that the Act applies within and outside Australia.
Clause 16 will provide that the Act is not intended to limit or exclude state and territory laws to the extent that those laws are capable of operating concurrently with the Act. The Explanatory Memorandum recognises the role of state and territory governments in regulating the operations of critical infrastructure and states that the Bill ‘does not seek to disrupt or override the operation of such laws’.  
Clause 17 will provide that the Act does not enable a power to be exercised to the extent that it would impair the capacity of a state to exercise its constitutional powers. The Explanatory Memorandum states: ‘Although this restriction exists by way of the Melbourne Corporation principle, including it in the Bill highlights the Government’s acknowledgement of this important principle’.

Issue: constitutionality and impact on states
While acknowledging the Government’s efforts to mitigate any constitutional impact, the NSW and SA Governments remain concerned about how the powers and functions in the Bill will be exercised, and the potential practical and legal consequences. Their primary concern in this respect is with the proposed ministerial directions power in clause 32, specifically instances where a Commonwealth minister uses that power to direct a state or state instrumentality to take particular action (or refrain from taking particular action) in relation to a state-owned critical infrastructure asset.

The NSW Government referred to and supported a proposal by the Victorian Government to exclude state owned and operated assets from the Bill (the Victorian Government did not make a public submission). It also recommended (in the alternative) that powers to prescribe and declare critical infrastructure assets (under clauses 9 and 51 respectively) and issue directions (under clause 32) should require the consent of the relevant state when exercised in relation to state government owned or operated assets.

Critical infrastructure assets
The Bill will apply to critical electricity, water and gas assets and critical ports. Additional assets may be prescribed by the Minister in rules (which will be publicly available) or declared by the Minister (but not made public).

79. Explanatory Memorandum, SCI Bill, p. 34.
80. Ibid.
81. NSW Government, Submission to AGD, Exposure Draft, op. cit., pp. 1–3; SA Government, Submission to the PJCIS, op. cit., p. 3.
82. NSW Government, Submission to AGD, Exposure Draft, op. cit., pp. 1–3.
Subclause 9(1) will provide that critical infrastructure asset means:

- a critical electricity asset
- a critical port
- a critical water asset
- a critical gas asset
- an asset declared (by the Minister) under clause 51 to be a critical infrastructure asset or
- an asset prescribed by the rules (which under clause 61, the Minister may make by legislative instrument).

The Minister will be able to make rules that provide that a specified electricity, water or gas asset, or a port, that would otherwise fall within the relevant definitions is not a critical infrastructure asset.83

Under clause 10, a critical electricity asset will be:

- a network, system, or interconnector, for the transmission or distribution of electricity to ultimately service at least 100,000 customers or
- an electricity generation station that is critical to ensuring the security and reliability of electricity networks or electricity systems in a State or Territory, in accordance with the rules.

Under clause 11, a critical port will be land that forms part of any of the 20 security regulated ports listed in that provision or a security regulated port prescribed by the rules.84

Under clause 5, a critical water asset will be a water or sewerage system or network that is used to ultimately deliver services to at least 100,000 water or sewerage connections under the management of a water utility.

Under clause 12, a critical gas asset will be:

- a gas processing facility that has a capacity of at least 300 terajoules per day or any other capacity prescribed by the rules
- a gas storage facility that has a maximum daily quantity of 75 terajoules per day or any other quantity prescribed by the rules85
- a network or system for the distribution of gas to ultimately service at least 100,000 customers or any other number of customers prescribed by the rules or
- a gas transmission pipeline that is critical to ensuring the security and reliability of a gas market, in accordance with the rules.

Peter Jennings and APGA raised the need for criticality to be based not just on the number of customers or connections an asset services or its capacity, but also the type of customer (for example, gas infrastructure has been included partly due to its importance as a fuel for electricity generation, and some assets may service a smaller number of customers, but provide power to defence or intelligence facilities).86 These submissions appear not to have taken account of the ability for the Minister to prescribe additional assets under subclause 9(2) and declare additional assets under clause 51 (both outlined below), and make rules providing that specific assets are not critical infrastructure assets under subclause 9(2).

83. Subclause 9(2) and clause 61 (rules).
84. The 20 ports listed are: Adelaide, Broome, Brisbane, Cairns, Christmas Island, Dampier, Darwin, Eden, Fremantle, Geelong, Gladstone, Hay Point, Hobart, Melbourne, Newcastle, Port Botany, Port Hedland, Rockhampton, Sydney Harbour and Townsville. Under clause 5, security regulated port will have the same meaning as in the Maritime Transport and Offshore Facilities Security Act 2003, that is, areas of a port intended for use either wholly or partly in connection with the movement, loading, unloading, maintenance or provisioning of security regulated ships included in a notice published in the Gazette (subsection 13(1)).
85. There appears to be an error in subclause 12(1)(b) of the SCI Bill; the Explanatory Memorandum indicates that this was intended to be gas storage facilities that have ‘a maximum daily quantity capacity of at least 75 terajoules per day’ [emphasis added]: Explanatory Memorandum, SCI Bill, p. 33.
86. Jennings, Submission to AGD, op. cit., p. 1; APGA, Submission to the PJCIS, op. cit., p. 7.
Issue: lack of certainty about what constitutes a critical infrastructure asset

Stakeholders raised several concerns relating to a lack of clarity about what constitutes different types of critical infrastructure asset, specifically:

- a lack of clarity in the Bill and the Explanatory Memorandum as to whether it is a water utility itself that is a critical water asset, or particular physical assets operated by a water utility (such as a water filtration plant, water main or pumping station)\(^{87}\)
- whether the reference to ‘ultimately servicing’ a particular number of customers/connections (used in definitions of critical water, electricity and gas assets) means an asset that actually services that many customers/connections, or one that has the capacity or capability to service them\(^{88}\)
- the breadth of definitions relating to critical infrastructure assets, for example, whether a rail network may be taken to be a critical electricity asset because of its role in distribution and\(^{89}\)
- whether critical port means the entire port or certain infrastructure within it.\(^{90}\)

Prescription of assets (public)

Clause 9 will allow the Minister to prescribe an asset as a critical infrastructure asset in rules if the Minister is satisfied that:

- the asset is critical to the social or economic stability of Australia or its people, the defence of Australia, or national security (Australia’s defence, security or international relations\(^{91}\)) and
- there is a risk, in relation to the asset, that may be prejudicial to security (within the meaning of the ASIO Act).\(^{92}\)

The Minister will be required to consult the First Minister of the state or territory in which the critical infrastructure is located and each minister in that state or territory who has responsibility for the regulation or oversight of the relevant industry (electricity, water, ports, gas or an industry prescribed by the rules).\(^{93}\) The Minister must invite each consulted minister to make written representations about the proposed prescription of the asset, within a specified period. The period specified will generally be required to be at least 28 days; however, the Minister will be able to specify a shorter period if he or she is satisfied that it is necessary because of urgent circumstances.

The Minister will be required to conduct those consultations and have regard to any representations made before prescribing an asset. Rules made under the Act will be legislative instruments and subject to parliamentary disallowance.\(^{94}\)

The NSW Government recommended that prescription of an asset owned or operated by a state government should require the consent of the relevant state, not just consultation, partly as a means to ensure that the Bill does not impair the capacity of the states to exercise their constitutional powers.\(^{95}\)

Issue: prescription of additional classes of assets

It is not obvious from the language used in clause 9; however, the Explanatory Memorandum indicates that the Government anticipates prescribing not only specific assets, but also classes of assets.\(^{96}\) This may allow the scope of the Act to be expanded significantly through rules made by the Minister. While those rules would be

---

87. SA Government, Submission to the PJCIS, op. cit., pp. 4, 7; Sydney Water, Submission to AGD, op. cit.; Hunter Water, Submission to AGD, op. cit.; WSAA, Submission to the PJCIS, op. cit.
88. TasWater, Submission to AGD, Exposure Draft, op. cit.
89. NSW Government, Submission to AGD, Exposure Draft, op. cit., p. 6. There is no indication that the Government intends to capture rail networks.
90. NT Government, Submission to AGD, Exposure Draft, op. cit., p. 6. It would appear to be the former.
91. National security is defined in clause 5.
92. Security is defined in clause 5. Except in clauses 10 and 12, where the term will take its ordinary meaning, security will have the same meaning as in the Australian Security Intelligence Organisation Act 1979 (ASIO Act) (section 4).
93. Relevant industry is defined in clause 5.
94. Clause 61.
subject to parliamentary disallowance, Parliament may wish to consider whether the expansion of the Act to additional classes of critical infrastructure assets would be more appropriately pursued through amendments to primary legislation.

Declaration of assets (not public)

Clause 51 will allow the Minister to declare a particular asset to be a critical infrastructure asset if:

- the asset is not otherwise a critical infrastructure asset
- the asset relates to a relevant industry and
- the Minister is satisfied that:
  - the asset is critical infrastructure that affects national security (Australia’s defence, security or international relations97) and
  - there would be a risk to national security if it were publicly known that the asset is critical infrastructure that affects national security.

A declaration must specify the entity that is the responsible entity for the asset. The Minister must notify each reporting entity for the asset and the First Minister of the state or territory in which the asset is located within 30 days of making the declaration; notices must specify the obligations of a reporting entity under the Act.98

Declarations will not be legislative instruments, and for reasons of national security, will not be made public.

Issue: lack of consultation requirements for declared assets

While the Minister will be required to notify the First Minister of the relevant state or territory after the fact, unlike the prescription of assets under clause 9, there will be no requirement for the Minister to consult state or territory ministers before declaring an asset to be a critical infrastructure asset under clause 51. While the declaration power under clause 51 will operate more narrowly than the prescription power under clause 9, it is not entirely clear why the Minister should not still be required to consult state or territory ministers before making a declaration, and this difference is not explained in the Explanatory Memorandum. This issue was raised in submissions to the Exposure Draft consultations from the NSW and SA Governments, with NSW explicitly recommending that consultation be required.99 The NSW Government also recommended that declaration of an asset owned or operated by a state government should require the consent of the relevant state, not just consultation, partly as a means to ensure that the Bill does not impair the capacity of the states to exercise their constitutional powers.100

Issue: whether the Bill should apply to additional sectors

As noted earlier in this Digest, the Shadow Assistant Minister for Cyber Security and Defence and some stakeholders have suggested that the Bill should apply to additional sectors, including health and medical facilities, the banking and finance sector and airports. The Department of Home Affairs’ submission to the PJCIS outlined the rationale for the application of the Bill to the electricity, gas, water and ports sectors and stated:

> While other critical infrastructure sectors, including banking and finance, health and aviation are at risk from espionage, sabotage and coercion, the level of existing regulation in place lowers their risk profile. The Centre will continue to work with these sectors through existing mechanisms including the Trusted Information Sharing Network (TISN) to improve their understanding of the threats of espionage, sabotage and coercion and to develop mitigation strategies.101

The Parliamentary Joint Committee on Intelligence and Security was satisfied that additional sectors did not need to be included in the Bill. However, it recommended that the Government review and develop measures to ensure that Australia has a continuous supply of fuel to meet its national security priorities, and as part of that

97. National security is defined in clause 5.
98. First Minister is defined in clause 5 to mean the Premier of a state or the Chief Minister of the ACT or NT.
100. NSW Government, Submission to AGD, Exposure Draft, op. cit., p. 1.
101. Department of Home Affairs, Submission to the PJCIS, op. cit., p. 6 (see pages 5–6 for details of how risk was assessed).
process should consider whether critical fuel assets should in future be made subject to the measures in the SCI Bill. 102

**Reporting entities and operators**

The concept of *reporting entities* is relevant to both of the key measures in the Bill. Reporting entities will be required to provide information to be kept on the register to be established by Part 2 of the Bill, and may be directed (as may *operators* of critical infrastructure assets) by the Minister to do certain things under Part 3.

*Reporting entities* for an asset will include the *responsible entity* for the asset and *direct interest holders* in relation to the asset. 103 In some cases, an entity will be both the responsible entity and a direct interest holder.

The *responsible entity* for an asset will be:

- the entity that holds the licence, approval or authorisation to operate a *critical electricity asset* or a *critical gas asset* to provide the service to be delivered by the asset
- the water utility that holds the licence, approval or authorisation under an Australian law to provide the service to be delivered by a *critical water asset*
- the port operator (within the meaning of the *Maritime Transport and Offshore Facilities Security Act 2003* 104) of a *critical port*
- for a critical infrastructure asset declared under clause 51, the entity specified in the declaration or
- for a critical infrastructure asset prescribed by the rules for the purpose of paragraph 9(1)(f), the entity specified in the rules. 105

An entity will be a *direct interest holder* in relation to an asset if it:

- holds a legal or equitable interest of at least 10 per cent in the asset (including interest held jointly with one or more other entities) or
- holds a lease of, or an interest in, the asset that puts the entity in a position to directly or indirectly influence or control the asset. 106

The *operator* of an asset will be:

- for a *critical port*, a port facility operator (within the meaning of the *Maritime Transport and Offshore Facilities Security Act 2003*) of a port facility within the port or
- for any other type of critical infrastructure asset, an entity that is authorised to operate the asset or part of the asset. 107

In some cases, an entity will be both the responsible entity for and an operator of an asset.

**Issue: definition of direct interest holder**

Stakeholders raised concerns relating to a lack of clarity about which entities will be *direct interest holders*, specifically:

- whether the intention is to capture only immediate shareholders or interest holders, or also intermediate or ultimate holding entities, of assets and108
- the references to influence and control in the definition might mean that it will capture financiers that have a certain level of influence or control over an asset, even where they have not enforced their security (the LCA


103. Clause 5.


105. Clause 5.

106. Subclause 8(1). Subclause 8(2) outlines how that provision applies to trusts, partnerships, superannuation funds that are trusts and unincorporated foreign companies.

107. Clause 5.

108. LCA, Submission to PJCIS, op. cit., p. 2; SA Government, Submission to the PJCIS, op. cit., pp. 4–5, 7; TransGrid, Submission to AGD, op. cit., p. 2.
recommended including ‘an express carve-out for money lending agreements’ based on that in the Foreign Acquisitions and Takeovers Regulation 2015).  

In its supplementary submission to the PJCIS, the Department of Home Affairs stated that it would seek to:

- amend definition of **direct interest holder** to clarify that it is ‘limited to the immediate shareholder or interest holder and does not extend to any intermediate or ultimate holding entities’
- include a definition of ‘influence and control’ and
- include a carve-out for money lenders modelled broadly on the one in the Foreign Acquisitions and Takeovers Regulation 2015.  

The Parliamentary Joint Committee on Intelligence and Security recommended that the SCI Bill and the Explanatory Memorandum be amended to more appropriately define **direct interest holder** in order to capture the intended range of ownership arrangements, and clarify:

- money lenders are not direct interest holders where they hold an interest through a financing arrangement and
- intermediate and ultimate holding entities are not direct interest holders.  

**Register of Critical Infrastructure Assets (Part 2)**

**Part 2** of the Bill will establish the Register of Critical Infrastructure Assets and require **reporting entities** to provide information that will be kept in the register.

**Establishment of the Register**

**Clauses 19–21** will require the Secretary to keep a register containing:

- information obtained under provisions requiring **reporting entities** to give information and notify the Secretary of certain events
- other **operational information** and **interest and control information** and
- any corrections or updates to such information.

**Clause 22** will require the Secretary to ensure that the register is not made public. **Division 3 of Part 4** of the Bill will set out how information obtained under **Part 2** may be dealt with and an offence for unauthorised use or disclosure.

**Information that must be provided by reporting entities initially**

**Clause 23** will require an entity that is, or will be, a **reporting entity** for a critical infrastructure asset at the end of the grace period, to give the Secretary certain information by the end of the grace period (six months) or 30 days after the day the entity becomes a reporting entity for the asset, whichever is later.

A reporting entity that is a **responsible entity** will be required to provide **operational information** in relation to the asset, that is:

- the location of the asset
- a description of the area the asset services
- for each **responsible entity** and **operator** of the asset: the name, ABN or other similar business number, the address of the head office or principal place of business and the country in which the entity was incorporated, formed or created
- the full name of the entity’s chief executive officer and the country or countries of which he or she is a citizen
- a description of the arrangements under which each operator operates the asset or part of the asset

---

109. LCA, **Submission** to PJCIS, op. cit., p. 3. Specifically, regulation 27 of the Foreign Acquisitions and Takeovers Regulation 2015.
110. Department of Home Affairs, **Supplementary submission** to the PJCIS, op. cit.
• a description of the arrangements under which data prescribed by the rules relating to the asset is maintained and
• any additional information prescribed by the rules.112

A reporting entity that is a direct interest holder must provide interest and control information in relation to the asset, that is:

• the name of the entity
• if applicable, the ABN or other similar business number of the entity
• for an entity other than an individual: the address of the head office or principal place of business and the country in which the entity was incorporated, formed or created
• for an entity that is an individual: the individual’s residential address, country in which he or she usually resides and the country or countries of which he or she is a citizen
• the type and level of interest the entity holds in the asset
• information about the influence or control the entity is in a position to exercise in relation to the asset, including decisions about the running of the asset and any person the entity has appointed to the body that governs the asset (and the ability of such persons to directly access networks or systems necessary for the operation or control of the asset)
• for each other entity in a position to directly or indirectly influence or control the first entity, the information in the first four points above and information about the influence or control it is in a position to exercise in relation to the first entity and
• any additional information prescribed by the rules.113

Ongoing obligations to provide information

Clause 24 will require reporting entities to provide certain information if a notifiable event occurs in relation to an asset.114 The information must be provided in the approved form and within 30 days of the event. Clause 26 will provide that an event is a notifiable event in relation to a critical infrastructure asset if:

• it has the effect that operational information or interest and control information previously obtained by the Secretary becomes incorrect or incomplete
• the event is an entity becoming a reporting entity for the asset or
• the event is a reporting entity for the asset becoming an entity to which the Act applies.115

Civil penalties

Civil penalties of up to 250 penalty units (currently $52,500) for a body corporate, or 50 penalty units (currently $10,500) for any other person, will apply for failing to comply with information obligations imposed by clauses 23 and 24.116

Exceptions and exemptions to obligations to provide information

Subclause 24(4) will provide that the requirement to provide information in relation to a notifiable event will not apply if, within 30 days of that event occurring, another notifiable event occurs and, as a result of the second event, information relating to the first event is no longer correct.

112. Operational information is defined in clause 7.
113. Interest and control information is defined in clause 6.
114. The table in subclause 24(3) sets out the particular information required in relation to different notifiable events, depending on the reporting entity.
115. The Explanatory Memorandum to the SCI Bill provides examples of events of each type (see pages 40–1).
116. The value of a penalty unit is set by section 4AA of the Crimes Act 1914, and is currently $210. Subsection 82(5) of the Regulatory Powers (Standard Provisions) Act 2014 provides that a pecuniary penalty imposed by a court must not be more than five times the penalty specified for a civil penalty provision if the person alleged to have contravened the provision is a body corporate; otherwise, it must not be more than the penalty specified for a civil penalty provision.
Clause 25 will provide that the initial obligation to provide information (under clause 23) or an obligation to provide information in relation to a notifiable event (under clause 24) does not apply to particular information if the person uses their best endeavours to obtain the information but is not able to do so.

Clause 27 will allow the rules to provide that Division 3 of Part 2, or specific provisions within it, do not apply in relation to any entity, specified classes of entities or specified entities. As noted earlier in this Digest, the Scrutiny of Bills Committee objected to this provision because it would allow the rules to amend the operation of primary legislation. It sought the Minister’s more detailed justification for the provision and advice as to whether it would be appropriate to amend the Bill to insert guidance about the making of rules for the purposes of clause 27.117

An entity wishing to rely on any of these exceptions or exemptions in proceedings for a civil penalty order for non-compliance will bear an evidential burden in relation to the matter (which would require adducing or pointing to evidence that suggests a reasonable possibility that the matter exists).118

Notification of change of reporting entities for assets declared under clause 51

If an entity is a reporting entity for an asset declared to be a critical infrastructure asset by the Minister under clause 51, it must notify the Secretary within 30 days if it ceases to be a reporting entity for the asset or if it becomes aware of another reporting entity for the asset.119 The notification must include that fact, and if another entity is a reporting entity, also the name of each other entity and the address of its head office or principal place of business (to the extent known).120 A civil penalty of up to 750 penalty units (currently $157,500) for a body corporate, or 150 penalty units (currently $31,500) for any other person, will apply for failing to comply with this notice requirement.121

Power for the Minister to issue directions (Part 3)

Part 3 of the Bill will establish the power for the Minister to issue directions to reporting entities and operators of critical infrastructure where there is a risk that is prejudicial to security that cannot otherwise be mitigated.

When a direction may be issued

Under clause 32, the Minister will be able to give a written direction to an entity that is a reporting entity for, or an operator of, a critical infrastructure asset requiring the entity to do, or refrain from doing, a specified act or thing within the period specified in the direction. A direction may only be given if:

• the Minister is satisfied that:
  – there is a risk of an act or omission that would be prejudicial to security in connection with the operation of, or the delivery of a service by, a critical infrastructure asset (subclause 32(1))
  – requiring the entity to do, or refrain from doing, a specified act or thing is reasonably necessary for purposes relating to eliminating or reducing that risk (subclause 32(3)(a))
  – reasonable steps have been taken to negotiate in good faith with the entity to achieve an outcome of eliminating or reducing that risk without a direction being given (subclause 32(3)(b)) and
  – no existing regulatory system of the Commonwealth, a state or a territory could be used instead (subclause 32(3)(d)) and

• an adverse security assessment in respect of the entity has been given to the Minister for the purposes of clause 32 (subclause 32(3)(c)).

Clause 5 will provide that adverse security assessment has the same meaning as in Part IV of the ASIO Act. ASIO’s functions include providing federal agencies and departments with security assessments relevant to their functions and responsibilities.122 An adverse security assessment in relation to a person is one that contains any opinion, advice or information that is or could be prejudicial to the interests of the person, and a

119. Clause 52.
120. Subclause 52(2). Subclause 52(3) will require the entity to use its best endeavours to determine the name and address.
121. Ibid.
122. ASIO Act, paragraph 17(1)(c) and section 37.
recommendation that prescribed administrative action be taken or not taken in respect of the person (where implementation of that recommendation would be prejudicial to the interests of the person). 123

Before giving a direction, the Minister must have regard to the matters set out in subclause 32(4) (such as the costs to the entity of complying with the direction and potential consequences for competition in the relevant industry and customers of or services provided by the entity) and may also have regard to any other relevant matter (subclause 32(5)(b)). The Minister must give the greatest weight to the adverse security assessment (subclause 32(5)(a)).

TransGrid suggested the inclusion of an additional safeguard whereby the time allowed for an entity to comply with a direction would be required to be reasonable ‘having regard to the nature of the direction and the steps required’. 124

**Consultation requirements**

**Clause 33** will require that before the Minister gives a direction, he or she must consult with the First Minister of the state or territory in which the critical infrastructure is located and each minister in that state or territory who has responsibility for the regulation or oversight of the relevant industry.

It will also require the Minister to give written notice of a proposed direction to the entity concerned and each consulted minister, inviting them to make written representations about the proposed direction within a specified period. The period specified will generally be required to be at least 28 days; however, the Minister will be able to specify a shorter period if he or she is satisfied that it is necessary because of urgent circumstances.

The NSW Government recommended that a direction related to an asset owned or operated by a state government should require the consent of the relevant state, not just consultation, partly as a means to ensure that the Bill does not impair the capacity of the states to exercise their constitutional powers. 125

**Review of decisions**

Adverse security assessments are subject to merits review under Division 4 of Part IV of the ASIO Act. However, section 38 of the ASIO Act allows the Attorney-General to issue a certificate in certain circumstances that prevents the subject of an adverse security assessment being notified of that assessment (and the subject’s right to seek a review). In her submission to the PJCIS, the IGIS pointed out:

> In this event, it would fall to the responsible entity to infer from the issuing of the Ministerial direction that it was the subject of an ASA (adverse security assessment), and to independently inform itself of its right to seek merits review of the ASA. This outcome could effectively deprive some responsible entities of an opportunity to exercise their review rights. It would yield no apparent benefit to security, as the making of the Ministerial direction would necessarily reveal the existence of the ASA. 126

The IGIS also put forward a possible solution to the issue:

> Adverse security assessments issued in connection with the Ministerial directions power in clause 32 of the Bill could be made subject to the separate notification requirements in section 38A of the ASIO Act, rather than the general notification requirements (and Ministerial certification-based exceptions) in section 38. The separate requirements in section 38A currently apply to ASAs that are issued in connection with certain Ministerial directions given under the Telecommunications Act 1997. Subsection 38A(3) of the ASIO Act does not allow a notice of the issuing of such an ASA to be withheld from the assessed entity. It permits only the exclusion of certain information from the copy of the assessment that is attached to the notice. 127

---

123. Ibid., subsection 35(1) (this subsection also includes a definition of prescribed administrative action that will be amended by the Consequential and Transitional Provisions Bill). See further the information on the 2010 ASIO Act Security Assessment Determination No. 2 (which does not appear to be publicly available) on page 67 of the Explanatory Memorandum to the SCI Bill.
124. TransGrid, Submission to AGD, op. cit., p. 3.
125. NSW Government, Submission to AGD, Exposure Draft, op. cit.,
126. IGIS, Submission to the PJCIS, op. cit., p. 3.
127. Ibid. Footnote references have been omitted from this quotation and can be viewed in the source document.
In its supplementary submission to the PJCIS, the Department of Home Affairs stated that it would seek to amend the Bill in line with the IGIS’s suggestion.\textsuperscript{128} The Parliamentary Joint Committee on Intelligence and Security recommended an amendment to this effect.\textsuperscript{129}

Decisions to issue directions under clause 32 will be reviewable under the Administrative Decisions (Judicial Review) Act 1977.

**Issue: thresholds for issue of directions and matters to be considered beforehand**

The NT Government and the LCA put forward additional matters that they suggest the Minister should be required to consider (under subclause 32(4)) before issuing a direction. The NT Government recommended that the Minister be required to consider the costs likely to be incurred by state and territory governments by an entity complying with the direction, and the likely implications of the direction on ‘economic and regional development, and future investment projects or supply chains’.\textsuperscript{130} The LCA noted that existing investors in critical infrastructure ‘often have negotiated existing contractual arrangements with the Commonwealth, State or Territory as to how assets would be operated or regulated’. It suggested that those existing arrangements either be protected from adverse modification ‘or at least be taken into account’ under subclause 32(4).\textsuperscript{131}

The LCA also suggested that the directions power only be available where the Minister is satisfied that there is a ‘substantial and imminent risk’ of ‘unauthorised interference with, or unauthorised access to, a critical infrastructure asset that would be prejudicial to security’ (a higher threshold than included in subclause 32(1) of being satisfied ‘that there is a risk of an act or omission that would be prejudicial to security’).\textsuperscript{132}

**Issue: interaction of directions power with other laws**

Energy Australia and TransGrid both raised the issue of how the directions power would interact with state and territory laws and other Commonwealth laws. Energy Australia suggested that the Bill provide that directions must not conflict with other laws, while TransGrid suggested the inclusion of a statutory immunity for entities that risk non-compliance with other laws ‘as a result of seeking to comply in good faith with a last resort direction’.\textsuperscript{133}

**Compliance and civil penalty**

Clause 34 will provide that an entity to which a direction has been issued under subclause 32(2) must comply with the direction. A civil penalty of up to 1,250 penalty units (currently $262,500) for a body corporate, or 250 penalty units (currently $52,500) for any other person, will apply for failing to comply with a direction. Clause 35 will provide an exception under which the obligation to comply with a direction will not apply to the extent that its operation would result in an acquisition of property from a person otherwise than on just terms. An entity wishing to rely on that exception in proceedings for a civil penalty order will bear an evidential burden in relation to the matter.

**Gathering and using information (Part 4)**

**Secretary’s powers to compel information and documents**

Clause 37 will allow the Secretary to issue a written notice to a reporting entity or an operator of a critical infrastructure asset requiring it to give information or produce documents (or copies of documents) within a specified period that the Secretary has reason to believe:

- is relevant to the exercise of a power, or performance of a duty or function, under the Act in relation to the asset or
- may assist with determining whether a power under the Act should be exercised in relation to the asset.

Before issuing a notice, the Secretary must have regard to the costs that would be likely to be incurred to comply with a notice, and may have regard to any other relevant matters. Subclause 37(6) will provide that an entity is

\textsuperscript{128} Department of Home Affairs, Supplementary submission to the PJCIS, op. cit.
\textsuperscript{130} NT Government, Submission to AGD, Exposure Draft, op. cit., p. 4.
\textsuperscript{131} LCA, Submission to the PJCIS, op. cit., p. 5.
\textsuperscript{132} LCA, Submission to the PJCIS, op. cit., pp. 6–7.
\textsuperscript{133} Energy Australia, Submission to AGD, op. cit.; TransGrid, Submission to AGD, op. cit., p. 3.
entitled to reasonable compensation for complying with a requirement to provide copies of documents. It is not clear why this does not extend to the costs of complying with requirements to provide information or produce documents.

A civil penalty of up to 750 penalty units (currently $157,500) for a body corporate, or 150 penalty units (currently $31,500) for any other person, will apply for failing to comply with a notice given under subclause 37(2) (see subclause 37(4)).

Clauses 38 and 39 will provide for the Secretary to make copies of and retain documents respectively. Clause 39 will allow the Secretary to retain documents ‘for as long as is necessary’.

Under clause 40, an entity will not be excused from providing information, documents or copies of documents on the basis that it might tend to incriminate them or expose them to a penalty (that is, the privilege against self-incrimination will not apply). If the entity is an individual, neither the information, nor information obtained as a direct or indirect consequence of giving the information, will be admissible in criminal proceedings (except for an offence of providing false or misleading information or documents related to the Act) or civil proceedings (except for recovery of a penalty for breaching subclause 37(4)) against the individual.

Issue: scope of notice and time for compliance

Clause 37 does not include a minimum period that the Secretary must give an entity to comply with a notice to produce information or documents. Minimum periods are usually stipulated, and the Government’s Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers recommends that notices be required to provide a person a minimum of 14 days to comply. 134

There is also no provision made for an entity to seek an extension of time to comply with a notice, or to seek any amendment to the scope of a notice (for example, if the entity does not have and is unable to obtain the requested information). Consideration could be given to the inclusion of mechanisms for an entity to request the issue of a revised notice or an extension of time (which the Secretary would then have discretion to refuse), or the insertion of a ‘reasonable excuse’ defence to the civil penalty in subclause 37(4) for failing to comply with a notice.

Authorised use and disclosure of protected information

Subdivision A, Division 3 of Part 4 of the Bill will set out the circumstances in which and purposes for which protected information may be used and disclosed. Subdivision B will create an offence for unauthorised use or disclosure—see further below.

Protected information will be defined in clause 5 to mean information in relation to an asset that:

• is obtained by a person in the course of exercising powers or performing duties or functions under the Act

• is the fact that the asset is declared to be a critical infrastructure asset under clause 51 (declarations made by the Minister that are not made public for reasons of national security) or

• was information of one of the types mentioned above, and is obtained by a person through an authorised disclosure or in accordance with an exception to the unauthorised disclosure offence.

An entity will be permitted to make a record of, use or disclose protected information for the purposes of exercising its powers or performing its functions or duties under the Act, or otherwise ensuring compliance with the Act (clause 41). 135

The Secretary will also be permitted to disclose protected information:

• to certain persons, and make a record of or use protected information for the purpose of that disclosure, for the purposes of enabling or assisting the other person to exercise their powers or perform their functions or duties (clause 42) and

• to an enforcement body (within the meaning of the Privacy Act 1988), for the purpose of enforcement related activities (clause 43).

---

134. AGD, A guide to framing Commonwealth offences, infringement notices and enforcement powers, AGD, September 2011, pp. 92–3.

135. Examples are provided on pages 73–4 of the Explanatory Memorandum to the SCI Bill.
The persons to whom the Secretary may disclose protected information under clause 42 will be:

- federal ministers with responsibility for national security, law enforcement, foreign investment, taxation policy, industry policy, promoting investment in Australia, defence and/or the regulation or oversight of the relevant industry for the critical infrastructure asset to which the information relates
- state or territory ministers with responsibility for regulation or oversight of the relevant industry for the critical infrastructure asset to which the information relates
- a person employed by one of those federal, state or territory ministers and
- the head of, or an officer or employee of, a department or agency administered by one of those federal, state or territory ministers.

Clause 44 will permit secondary use and disclosure of information for the purposes for which it was initially disclosed.

Issue: Secretary’s powers to share protected information

Some industry stakeholders raised concerns about the Secretary’s powers to share protected information for purposes other than the measures in the Bill. TasWater considered that clause 42 is too broad:

These powers of disclosure do not specifically reference the performance of functions or duties under any particular legislation, but simply reference “powers” and “functions or duties”.

In addition, the Secretary has an unfettered discretion as to whether disclosure is made, with no guiding principles, parameters or issues to be considered in the exercise of that discretion.136

AusGrid and Energy Australia considered that given the sensitive nature of the information, provision should be made to ensure its security when shared, with Ausgrid recommending that before making a disclosure under clause 42, the Secretary be required to be satisfied that there are systems and processes in place to ensure the security of any protected information.137

Unauthorised use and disclosure of protected information

It will be an offence under clause 45 for an entity to make a record of, disclose or otherwise use protected information except as authorised under Subdivision A, Division 3 of Part 4, or as required by subclause 51(3) or subclause 52(4) (under which the Minister and the Secretary respectively must notify certain persons of the declaration of an asset as a critical infrastructure asset). The maximum penalty will be imprisonment for two years and/or 120 penalty units (currently $25,200) for an individual and 600 penalty units (currently $126,000) for a body corporate.138 This is the only criminal offence in the Bill.

Clause 46 will provide for three exceptions to the offence, specifically where the making of a record, disclosure or use was:

- required or authorised under another Commonwealth law or a state or territory law prescribed by the rules
- done in good faith and in purported compliance with Subdivision A, Division 3 of Part 4, subclause 51(3) or subclause 52(4) or
- disclosed to the entity to whom it relates, where it relates to the entity itself, or where it is made with the consent of the entity to whom the information relates.

An entity wishing to rely on any of these exceptions in proceedings for an offence against clause 45 will bear an evidential burden in relation to the matter (which would require adducing or pointing to evidence that suggests a reasonable possibility that the matter exists).139

136. TasWater, Submission to AGD, op. cit., p. 2.
137. Ausgrid, Submission to AGD, op. cit.; Energy Australia, Submission to AGD, op. cit., p. 2.
138. Subsection 4B(3) of the Crimes Act provides that where a body corporate is convicted of a Commonwealth offence, unless the contrary intention appears, the court may impose a penalty of up to five times the maximum penalty for an individual. Clauses 54–56 will set out how the Act applies to partnerships, trusts and superannuation funds that are trusts, and unincorporated foreign companies. For the application of offences, see subclauses 54(3), 55(2) and (3) and 56(3).
Clause 47 will provide that an entity is not to be required to disclose protected information to a court, tribunal or other person except where necessary for the purposes of the Act. The NSW Government questioned whether this provision might contravene principles established in Kable v Director of Public Prosecutions and section 75 of the Constitution (original jurisdiction of the High Court), but did not provide any further detail on the nature of its concerns.\(^\text{140}\)

**SCI Bill: other provisions**

**Enforcement (Part 5)**

Part 5 of the SCI Bill will provide that civil penalty provisions in the Bill are enforceable under Parts 4, 6 and 7 of the Regulatory Powers Act. If a civil penalty provision of the Act is contravened, the Minister or the Secretary will be able to:

- apply to a relevant court for a civil penalty order requiring a person to pay a pecuniary penalty (under Part 4 of the Regulatory Powers Act)
- accept an undertaking relating to compliance with a civil penalty provision that may be enforced through an order of a relevant court (under Part 6 of the Regulatory Powers Act) and/or
- apply to a relevant court for an injunction (under Part 7 of the Regulatory Powers Act).

**Administrative provisions (Part 7)**

**Application to certain entities**

Division 2 of Part 7 of the Bill will set out how it applies to partnerships (clause 54), trusts and superannuation funds that are trusts (clause 55) and unincorporated foreign companies (clause 56).

**Secretary’s powers**

Division 3 of Part 7 of the Bill will:

- provide the Secretary the explicit power to undertake an assessment of a critical infrastructure asset to determine if there is a risk to national security relating to the asset (clause 57)
- provide that the Secretary must notify a reporting entity in writing if he or she becomes aware that an asset has ceased to be a critical infrastructure asset (clause 58) and
- allow the Secretary to delegate any of his or her powers, functions or duties to an SES employee or acting SES employee of the Department, by written instrument (clause 59).

**Annual reports**

Clause 60 will require the Secretary to prepare a report on the operation of the Act for each financial year and provide it to the Minister for presentation to the Parliament. Each report must ‘deal with’ the number of notifications made to the Secretary of notifiable events (under Division 3 of Part 2), any directions given by the Minister under clause 32, the use of powers to compel information (under Division 2 of Part 4), any enforcement action against an entity (under Part 5 and the Regulatory Powers Act) and the number of declarations of assets as critical infrastructure assets by the Minister under clause 51. The Minister must table the report in each house of Parliament within 15 sitting days of receiving it.\(^\text{141}\)

**Rules**

Clause 61 will provide that the Minister may make rules for the purposes of the Act by legislative instrument. The rules may not do certain things, such as creating offences or civil penalties or providing certain coercive powers.

---

\(^{140}\) NSW Government, Submission to AGD, Exposure Draft, op. cit., p. 4.

\(^{141}\) Acts Interpretation Act 1901, subsection 34C(3).
Consequential and Transitional Provisions Bill

Consequential amendments

Section 35 of the ASIO Act contains definitions for the purposes of Part IV of that Act, which relates to ASIO’s security assessment function. Item 1 of Schedule 1 will amend the definition of prescribed administrative action in subsection 35(1) of the ASIO Act to include the exercise of a power under subsection 32(2) of the Security of Critical Infrastructure Act. This will allow ASIO to provide the Minister with security assessments to inform the exercise of the directions power in clause 32 of the SCI Bill.

Subsection 122(1) of the FATA provides that a person may disclose protected information (as defined in section 120 of the FATA) to Commonwealth ministers and agencies responsible for certain Acts, for the purposes of administering those Acts. Item 2 of Schedule 1 will add the Security of Critical Infrastructure Act to the list of Acts in subsection 122(1). Subsections 122(2) and (3) of the FATA allow a person to disclose protected information to a Commonwealth minister or secretary of a department (respectively) responsible for certain matters (including, for example, agriculture and taxation policy), for the purpose of enabling the Minister to discharge those responsibilities. Item 3 of Schedule 1 will amend those subsections to add national security to the lists of matters.

Other amendments

Schedule 2 will make equivalent amendments to section 122 of the FATA as those made by items 2 and 3 of Schedule 1, but in relation to the Defence Act 1903 (for subsection 122(1)) and defence (for subsections 122(2) and (3)).

© Commonwealth of Australia

Creative Commons

With the exception of the Commonwealth Coat of Arms, and to the extent that copyright subsists in a third party, this publication, its logo and front page design are licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Australia licence.

In essence, you are free to copy and communicate this work in its current form for all non-commercial purposes, as long as you attribute the work to the author and abide by the other licence terms. The work cannot be adapted or modified in any way. Content from this publication should be attributed in the following way: Author(s), Title of publication, Series Name and No, Publisher, Date.

To the extent that copyright subsists in third party quotes it remains with the original owner and permission may be required to reuse the material.

Inquiries regarding the licence and any use of the publication are welcome to webmanager@aph.gov.au.

Disclaimer: Bills Digests are prepared to support the work of the Australian Parliament. They are produced under time and resource constraints and aim to be available in time for debate in the Chambers. The views expressed in Bills Digests do not reflect an official position of the Australian Parliamentary Library, nor do they constitute professional legal opinion. Bills Digests reflect the relevant legislation as introduced and do not canvass subsequent amendments or developments. Other sources should be consulted to determine the official status of the Bill.

Any concerns or complaints should be directed to the Parliamentary Librarian. Parliamentary Library staff are available to discuss the contents of publications with Senators and Members and their staff. To access this service, clients may contact the author or the Library’s Central Enquiry Point for referral.

Members, Senators and Parliamentary staff can obtain further information from the Parliamentary Library on (02) 6277 2500.