Australian Government
Department of Home Affairs

CRITICAL INFRASTRUCTURE CENTRE

Security Legislation Amendment (Critical Infrastructure) Bill 2020

Explanatory Document

November 2020

GLOSSARY

AAT – Administrative Appeals Tribunal

ACMA – Australian Media and Communications Authority

ACSC – Australian Cyber Security Centre

AEMO – Australian Energy Market Operator

APRA – Australian Prudential Regulation Authority

ASA – Australian Shareholders' Association

ASIC – Australian Securities and Investments Commission

ASIO – Australian Security Intelligence Organisation

ASIO Act – *Australian Security Intelligence Organisation Act 1979*

ATSA – *Aviation Transport Security Act 2004*

CESAR – Cyber Enhanced Situational and Response

Criminal Code – *Criminal Code Act 1995*

DISP – Defence Industry Security Program

FATA – *Foreign Acquisitions and Takeovers Act 1975*

FIRB – Foreign Investment Review Board

Home Affairs – Department of Home Affairs

IGIS – Inspector-General of Intelligence and Security

IS Act – *Intelligence Services Act 2001*

MTOFSA – *Maritime Transport and Offshore Facilities Security Act 2003*

MW – megawatts

NEM – National Energy Market

Privacy Act – *Privacy Act 1988*

PSPF – Protective Security Policy Framework

RBA – Reserve Bank of Australia

Register – Register of Critical Infrastructure Assets

Regulatory Powers Act – *Regulatory Powers (Standard Provisions) Act 2014*

SOCI Act – *Security of Critical Infrastructure Act 2018*

SCADA – Supervisory control and data acquisition

TEQSA – Tertiary Education Quality and Standards Agency

TSSR – Telecommunications sector security reforms contained in the *Telecommunications and Other Legislation Amendment Act 2017*

SECURITY LEGISLATION AMENDMENT (CRITICAL INFRASTRUCTURE) BILL 2020

GENERAL OUTLINE

1. The Australian Government is committed to protecting the essential services all Australians rely on by uplifting the security and resilience of our critical infrastructure. As the threats and risks to Australia's critical infrastructure evolve in a post-COVID world, so too must our approach to ensuring the ongoing security and resilience of these assets and the essential services they deliver.

2. Critical infrastructure is increasingly interconnected and interdependent, delivering efficiencies and economic benefits to operations. However, connectivity without proper safeguards creates vulnerabilities that can deliberately or inadvertently cause disruption and result in cascading consequences across our economy, security and sovereignty.

3. Threats ranging from natural hazards (including weather events) to human induced threats (including interference, cyber attacks, espionage, chemical or oil spills, and trusted insiders) all have the potential to significantly disrupt critical infrastructure. Recent incidents such as compromises of the Australian parliamentary network, university networks and key corporate entities, natural disasters and the impacts of COVID-19 illustrate that threats to the operation of Australia's critical infrastructure assets continue to be significant. Further, the interconnected nature of our critical infrastructure means that compromise of one essential function can have a domino effect that degrades or disrupts others.

4. The consequences of a prolonged and widespread failure in the energy sector, for example, could be catastrophic to our economy, security and sovereignty, as well as the Australian way of life, causing:

    - shortages or destruction of essential medical supplies;
    - instability in the supply of food and groceries;
    - impacts to water supply and sanitation;
    - impacts to telecommunications networks that are dependent on electricity;
    - the inability of Australians to communicate easily with family and loved ones;
    - disruptions to transport, traffic management systems and fuel;
    - reduced services or shutdown of the banking, finance and retail sectors; and
    - the inability for businesses and governments to function.

5. While Australia has not suffered a catastrophic attack on critical infrastructure, we are not immune:

    - over the last two years, we have seen several cyber attacks in Australia that have targeted the Federal Parliamentary Network, as the transport and education sectors;
    - malicious actors have taken advantage of the pressures COVID-19 has put on the health sector by launching cyber attacks on health organisations and medical research facilities; and
    - key supply chain businesses transporting groceries and medical supplies have also been targeted.

6. Accordingly, Government will introduce an enhanced regulatory framework, building on existing requirements under the SOCI Act. The Security Legislation Amendment (Critical Infrastructure) Bill 2020 gives effect to this framework by introducing:

    - a Positive Security Obligation for critical infrastructure, including a risk management program, to be delivered through sector-specific requirements, and mandatory cyber incident reporting;

    - enhanced cyber security obligations for those assets most important to the nation, described as systems of national significance; and

    - government assistance to relevant entities for critical infrastructure sector assets in response to significant cyber attacks that impact on Australia's critical infrastructure assets.

7. These changes will be underpinned by enhancements to Government's existing education, communication and engagement activities, under a refreshed Critical Infrastructure Resilience Strategy. This will include a range of activities that will improve our collective understanding of risk within and across sectors.

8. The enhanced framework will uplift security and resilience in all critical infrastructure sectors. When combined with better identification and sharing of threats, this framework will ensure that Australia's critical infrastructure assets– whether industry or government owned and operated – are more resilient and secure. Government will work in partnership with responsible entities of critical infrastructure assets to ensure the new requirements build on and do not duplicate existing regulatory frameworks.

9. This framework will apply to owners and operators of critical infrastructure regardless of ownership arrangements. This creates an even playing field for owners and operators of critical infrastructure and maintains Australia's existing open investment settings, ensuring that businesses who apply security measures are not at a commercial disadvantage.

10. The Australian Government's Critical Infrastructure Resilience Strategy currently defines 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.'

11. Within that broad definition of critical infrastructure, the SOCI Act currently places regulatory obligations on specific entities in the electricity, gas, water and maritime ports sectors. However, as the security landscape evolves, so must our approach to managing risk across all critical infrastructure sectors.

12. As such, the amendments in this Bill will enhance the obligations in the SOCI Act, and expand its coverage to the following sectors: communications; financial services and markets; data storage and processing; defence industry; higher education and research; energy; food and grocery; health care and medical; space technology; transport; and water and sewerage.

13. Further details on each of the critical infrastructure sectors and associated critical assets, definitions and the basis for their inclusion in these reforms is outlined at Part 1 – Sector Thresholds.

The reforms

14. The Commonwealth needs to establish a clear, effective, consistent and proportionate approach to ensuring the resilience of Australia's critical infrastructure. The amendments to the SOCI Act will drive the uplift of the security and resilience of Australia's critical infrastructure.

15. The Security Legislation Amendment (Critical Infrastructure) Bill 2020 (the Bill) will introduce an all-hazards Positive Security Obligation for a range of critical infrastructure assets across sectors. This ensures industry is taking the appropriate steps to manage the security and resilience of their assets. The specific matters to be included in a critical infrastructure risk management program will be prescribed in rules, which will be co-designed between industry and government.

16. The Bill also recognises those assets that are the most critical to the security, economy and sovereignty of Australia. These 'systems of national significance' will bear additional cyber obligations recognising the cyber threat environment we currently face. Finally, while these measures are designed to ensure we do not suffer a catastrophic cyber attack, the Bill will ensure Government has the necessary powers to provide direct assistance to industry in the event of a serious cyber security incident.

Positive Security Obligation

17. The Positive Security Obligation will build on the existing obligations in the SOCI Act to embed preparation, prevention and mitigation activities into the business as usual operating of critical infrastructure assets, ensuring that the resilience of essential services is strengthened. It will also provide greater situational awareness of threats to critical infrastructure assets.

18. The Positive Security Obligation involves three aspects:

    - adopting and maintaining an all-hazards critical infrastructure risk management program;
    - mandatorily report serious cyber security incidents to the Australian Signals Directorate (ACSC); and
    - where required, providing ownership and operational information to the Register of Critical Infrastructure Assets.

19. Importantly, each aspect of the Positive Security Obligation will only apply once a rule is made in relation to that aspect for a critical infrastructure asset or class of critical infrastructure assets. The rules will prescribe which aspects are 'switched on' for a critical infrastructure asset or class of critical infrastructure assets.

20. The critical infrastructure risk management program will require responsible entities of critical infrastructure assets to manage and mitigate risks. Responsible entities of critical infrastructure assets will be required to take an all-hazards approach when identifying and understanding those risks – both natural and human induced hazards.

21. Partnerships with industry sit at the foundation of this measure. Government and industry stakeholders will work together to co-design the sector-specific requirements which will underpin the risk management program obligation. The co-design process will develop a clear set of requirements for each of the regulated sectors, which:

    - recognise and do not duplicate existing regulatory or non-regulatory approaches across sectors;
    - are principles-based and proportionate to the risk profile of the particular sector; and
    - impose the least regulatory burden necessary to achieve the security outcomes.

22. Responsible entities of critical infrastructure assets will be required to report serious cyber security incidents to the relevant Commonwealth body. The objective of this reform is to collect information which will support the development of an aggregated threat picture and comprehensive understanding of cyber security risks to critical infrastructure in a way that is mutually beneficial to Government and industry. This will better inform both proactive and reactive cyber response options – ranging from providing immediate assistance to industry to working with industry to uplift broader security standards.

23. Part 2 of the current SOCI Act requires assets covered by the Act to provide ownership and operational information to the Secretary of Home Affairs. This information is held on the Register of Critical Infrastructure Assets (the Register). The Bill will extend this requirement to the expanded class of critical infrastructure assets where appropriate (for example, it may not be necessary where information is being collected under an equivalent regime for certain assets).

24. The increased range of sectors covered by the Register will enable the Government to develop and maintain a comprehensive picture of national security risks, and apply mitigations where necessary. Analysis of the information in the Register will enable the Critical Infrastructure Centre to:

    - assess ultimate ownership, and therefore influence and control over, critical infrastructure assets;
    - analyse interdependencies among critical infrastructure assets and sectors; and
    - identify commonalities in services being used by critical infrastructure assets, such as shared IT service providers or shared control systems.

25. The successful delivery of all aspects of the Positive Security Obligation is predicated on the identification of sector-specific regulators to manage the implementation and compliance of these elements of the reforms. The Department of Home Affairs, or other relevant Commonwealth regulator prescribed in the rules, will be provided with the standard monitoring and investigation powers under the *Regulatory Powers (Standard Provisions) Act 2014* to support compliance and enforcement activities.

26. Regulators will adopt a risk-based approach to developing and enforcing the Positive Security Obligation. Sector regulators will work with entities to ensure the Positive Security Obligation is applied in a proportionate and reasonable manner, taking into account the needs and existing capabilities of each sector. Regulators will have a role in monitoring and enforcing compliance while seeking to minimise the economic and operational impact on businesses.

Enhanced Cyber Security Obligations for systems of national significance

27. The Enhanced Cyber Security Obligations in the Bill will support a bespoke, outcomes-focused partnership between Government and Australia's most critical assets – privately declared as 'systems of national significance'. These obligations will enhance the already mature Government-industry information sharing arrangements to build an aggregated threat picture and comprehensive understanding of cyber security risks to critical infrastructure in a way that is mutually beneficial to Government and industry.

28. Systems of national significance are a significantly smaller subset of critical infrastructure assets that, by virtue of their interdependencies across sectors and cascading consequences of disruption to other critical infrastructure assets and critical infrastructure sectors, are crucial to the nation.

29. Under the Enhanced Cyber Security Obligations, the Secretary of Home Affairs may require the responsible entity for a system of national significance to undertake one or more prescribed cyber security activities. These include the development of cyber security incident response plans, cyber

security exercises to build cyber preparedness, vulnerability assessments to identify vulnerabilities for remediation, and provision of system information to build Australia's situational awareness. The Bill explicitly requires the Secretary of Home Affairs to request the prescribed activity in order to ensure activities have a clear, stated security objective.

30. Through consultation in developing this Bill, stakeholders provided support for greater threat information sharing and partnerships with Government. The Enhanced Cyber Security Obligations will support the sharing of near-real time threat information to provide industry with a more mature understanding of emerging cyber security threats, and the capability to reduce the risks of a significant cyber attack against Australia's most critical assets.

Government Assistance

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

32. During consultation, stakeholders were broadly supportive of the Government actively protecting critical infrastructure in exceptional circumstances, while calling for clearly defined safeguards and oversight mechanisms. The Government Assistance powers in the Bill are clearly defined and are confined, proportionate and appropriate. Further details on the scope of powers and safeguards are outlined in Part 3A of the Bill.

Consultation

33. Over a five week period from 12 August 2020, the Department of Home Affairs on behalf of the Australian Government, undertook an extensive consultation process. During this period the Department met with over 2,000 people from over 540 entities across all affected sectors, peak bodies and states and territories, and received 194 submissions.

34. Consultation revealed cautious support for an enhanced regulatory framework for Australia's critical infrastructure while noting:

- the need for genuine co-design of sector-specific requirements and recognition that voluntary partnerships remain the first preference for resolving incidents;
- the need for greater clarity around how critical infrastructure assets and systems of national significance are to be defined;
- concern over the extent of the proposed Government Assistance powers;
- the unclear and possibly high regulatory impost, as well as possible duplication with existing regulatory frameworks (particularly in sectors with existing, mature security frameworks); and
- the risks in pursuing the reforms on an expedited timeframe.

35. Feedback received during consultation has informed the development of an exposure draft Bill.

36. Further engagement on the exposure draft legislation, coupled with ongoing stakeholder co-design, a continued emphasis on cooperative partnerships and graduated implementation of sector-specific obligations, will minimise regulatory burden, and manage industry and jurisdictions' concerns.

Voluntary engagement through the Trusted Information Sharing Network

37. Increased engagement and education will underpin the success of the regulatory reforms outlined above. The Trusted Information Sharing Network for Critical Infrastructure Resilience was established in 2003 and remains the primary voluntary engagement mechanism for business-government information sharing and resilience building initiatives. However, in recent years industry has sought greater value from this mechanism.

38. The Government will enhance the existing Trusted Information Sharing Network by co-designing with industry a new fit-for-purpose engagement mechanism that allows for greater cross-sector collaboration in preparing for and responding to the evolving environment. The refreshed engagement mechanism will ensure industry participants can discuss resilience issues which impact Australia's critical infrastructure which will increase participation by owners and operators of critical infrastructure, supply chain entities and state and territory governments.

39. The new engagement mechanism will be a channel for developing and communicating critical infrastructure resilience information and a forum to co-design sector-specific obligations and best practice guidance. This approach will encourage all affected responsible entities, large and small, to participate in their design and ensure the resulting obligations provide a level playing field for all participants. The new engagement mechanism will also be used to inform the new Critical Infrastructure Resilience Strategy (due for release in early 2021), capturing lessons learned from crises this year including COVID-19.

Regulatory Impact Statement (RIS)

40. Government heard from the public consultation period that while there was broad in-principle support for the introduction of the reforms, industry were keen to see genuine co-design of the sector-specific requirements to ensure the minimisation of regulatory duplication and subsequent costs to industry. Government agrees that co-design with industry and understanding the costs and benefits of all options available to achieve Government policy objectives is critical to the success of the reforms.

41. To date, the Government has conducted a qualitative Regulation Impact Statement which assesses the potential costs and benefits of the proposed reforms. Alongside introduction of legislation into Parliament, Government will outline the quantitative costs and benefits of the components of the reforms that will have a regulatory impact upon commencement, including:

    - the Enhanced Cyber Security Obligations (incident response plans, scenario based exercises, vulnerability assessments and access to system information);

    - the expansion of the existing register of critical infrastructure assets and the Ministerial directions power to the revised critical infrastructure sectors; and

    - mandatory cyber incident reporting.

42. Government will develop a more detailed Regulation Impact Statement with quantitative costs and benefits of the Positive Security Obligation risk management program when the sector-specific rules are being developed. The Government will develop these quantitative costs and benefits alongside industry and states and territories. Government will do this through a range of sector-specific workshops and engagements to ensure that the mechanisms already in place securing critical infrastructure are not duplicated.

43. There are a range of benefits expected to flow from these reforms. These benefits have been central to the design and development of the reforms. Specifically, the reforms are designed to ensure that all Australians will benefit through increased critical infrastructure resilience. The estimated high level benefits of the proposed regulatory reforms will:

- safeguard Australia's economy, sovereignty, and security by increasing critical infrastructure resilience against all hazards and making all hazard risk management practices part of doing business in Australia;

- provide certainty for businesses across all critical infrastructure sectors by setting clear security standards and creating a level playing field in the Australian market;

- align with business and community expectations for Government to take proportionate action when required to protect the essential services all Australians rely upon and safeguard Australia's sovereignty, economy and security more broadly;

- drive an improved all hazards management across supply chains, lifting resilience more broadly across the Australian economy and making all hazard management part of doing business in Australia;

- enable the Government to acquire near real-time cyber situational awareness from high criticality entities, allowing the Government to respond effectively and efficiently to emergencies and support business and the Australian economy and security;

- offer a level playing field for domestic and foreign investors with all aspects of the reforms being ownership agnostic;

- provide business with access to Government risk information, expertise and advice on the cyber threat environment and best practice security measures, through advice prepared by the ACSC.

- support business with guidance and advice from Government and fellow industry participants on security practices facilitated through a revitalised Trusted Information Sharing Network; and

- provide industry direction and support to be able to rapidly respond in the event of a significant cyber incident.

44. However, Government also recognises there are potential costs associated with an introduction of regulatory reform.

45. The Government will continue to work with industry and state and territory governments to make sure that existing regulations, frameworks and guidelines are leveraged, and to minimise any duplication or unnecessary cost burden. Close co-design will be integral to understanding the most effective way to implement the proposed reforms, and ensure the impost to industry is well understood and balanced against Government's policy objectives to uplift critical infrastructure resilience and security against all hazards.

PART 1—SECTOR AND CRITICAL INFRASTRUCTURE ASSET THRESHOLDS

46. The Bill introduces a range of new powers, including three key definitions to clearly outline who is covered by each of the powers in the SOCI Act.

- **Critical infrastructure sector (new section 8D)** – Definitions for each of the eleven critical sectors set the outer bounds of the SOCI Act and will perform two key functions:
    - The Minister for Home Affairs will only be able to prescribe or declare critical infrastructure assets, additional to those already provided in the legislation, from these sectors, and
    - The Government Assistance powers will only be able to be exercised in relation to entities in these sectors.
- **Critical infrastructure asset (amended section 9)** – Building on the existing definition in the SOCI Act, definitions of critical infrastructure assets within each of the eleven critical sectors will be introduced while retaining the Minister for Home Affairs' existing ability to prescribe or declare additional assets from these sectors when the Minister for Home Affairs is satisfied the asset is critical to the social or economic stability of Australia or its people, the defence of Australia or national security.

  The primary function of this definition is to outline the classes of assets to whom the Positive Security Obligation in the SOCI Act may apply. It is proposed that responsible entities for these assets will also fall within the proposed new definition of 'national security business' in the *Foreign Investment Reform (Protecting Australia's National Security) (National Security Business) Regulations 2020*, as indicated in the exposure draft of those regulations.

  Critical infrastructure assets across each sector have been identified through an assessment of whether, if destroyed, degraded, or rendered unavailable, there would be a significant detrimental impact on:
    - maintaining basic living standards for the Australian population – this includes those essential services and other services without which the safety, health or welfare of the Australian community or a large section of the community would be endangered or seriously prejudiced;
    - industries, commercial entities and financial institutions that underpin Australia's wealth and prosperity;
    - the security of large or sensitive data holdings which, if undermined, could lead to the theft of personal or commercially sensitive information, intellectual property or trade secrets; and
    - national security and defence capabilities.
- **Systems of national significance (new section 52B)** – The Minister for Home Affairs will have the power to declare a critical infrastructure asset as a 'system of national significance', having regard to the nature and extent of interdependencies with other critical infrastructure assets. Systems of national significance will be subject to the enhanced cyber security obligations in new Part 2C.

47. These reforms will leverage existing mechanisms and where necessary, build on them to deliver a more consistent approach to managing risk across all sectors. This will be achieved through, for

example, deferring to existing regulatory obligations where they are equivalent to components of the risk management obligations under the SOCI Act.

48. The Department of Home Affairs has consulted with representatives across the eleven critical infrastructure sectors to determine the application of the enhanced framework. Based on this consultation process, and analysis conducted by Home Affairs, the parameters for the definitions of critical infrastructure sectors and critical infrastructure assets have been developed, as outlined below.

COMMUNICATIONS

Sector definition

49. The Bill introduces a definition of the 'communications sector'. Entities that fall within the sector definition will be covered by the government assistance measures.

50. The sector definition reflects the infrastructure that is key to supporting telecommunications and broadcasting services, and the stability and security of the .au domain name system. The definition is also intended to be flexible so that it continues to be relevant as technology and infrastructure in this sector evolves.

51. The 'communications sector' is defined as the sector of the Australian economy that involves:

- supplying a carriage service; or
- providing a broadcasting service; or
- owning or operating assets that are used in connection with the supply of a carriage service; or
- owning or operating assets that are used in connection with the transmission of a broadcasting service; or
- administering an Australian domain name system.

52. The sector definition aims to capture all entities involved in supplying a carriage service or providing a broadcasting service, and the maintenance and operation of assets located in Australia which are used in connection with these services. This includes:

- carriers such as owners and operators of telecommunication networks, submarine cables, and satellites;
- carriage service intermediaries such as mobile service retailers;
- carriage service providers including internet service providers and mobile service providers;
- national broadcasters, commercial radio and television broadcasters; and
- owners and operators of broadcasting assets or facilities such as independent playout facilities, transmission and retransmission sites.

53. The sector definition also captures all entities involved in administering the Australian domain name system, specifically the .au namespace. This includes registries and registrars operating physical assets located within Australia.

Critical infrastructure asset definition

54. The Bill will introduce definitions for three types of critical infrastructure assets in this sector: telecommunications, broadcasting transmission, and domain name systems. Assets that fall within these definitions may be subject to each of the Positive Security Obligation:

    - the requirement to adopt and maintain a risk management program (Part 2A), in the event that the asset is specified in the rules under section 30AB to require such a program for this class of assets.

    - mandatory reporting of serious cyber security incidents, in the event that the asset is specified in the rules under section 30BB to require this for this class of assets.

    - providing ownership and operator information, in the event that the asset is specified in the rules under section 18A to require this for this class of assets.

55. The responsible entity for each of the assets (outlined below) is the entity that will be required to comply with each of the above obligations, if turned on.

Critical telecommunications asset

56. The Bill introduces a definition of a 'critical telecommunications asset'. The definition mirrors the assets currently regulated under the TSSR.[1] A 'critical telecommunications asset' is defined as:

    - a telecommunications network or facility which is owned or operated by a carrier and is used to supply a carriage service; or

    - a telecommunications network, or any other asset, that is owned or operated by a carriage service provider and used in connection with the supply of a carriage service.

57. Telecommunications infrastructure subject to the TSSR play an important role in supporting Australia's critical infrastructure and provide essential communications services including the emergency call service (Triple Zero and 112).

58. This definition will cover the networks that carry voice and data between users across Australia, and our connection with the rest of the world and space. This includes wires, fibre, towers, sensors, satellites, radio spectrum and physical infrastructure such as cable landing stations. However, the definition does not include Over-the-Top applications which operate over the top of this infrastructure (for example, Netflix and Skype).

Responsible entity

59. For a 'critical telecommunications asset', the responsible entity is the carrier that holds the carrier licence for the telecommunications network; or an entity that is the carriage service provider within the meaning of the *Telecommunications Act 1997*; or, if applicable, another entity that is prescribed by the rules in relation to the asset. This is appropriate as that will be the entity best placed to manage the day-to-day operations of the asset, and therefore ensure security and resilience of the asset in line with this regime.

60. The Department of Home Affairs acknowledges that the TSSR framework is currently under review as part of the Parliamentary Joint Committee on Intelligence and Security's 'Review of Part 14 of the Telecommunications Act 1997'. The outcomes of that review will inform how the Positive Security Obligation is implemented for the critical telecommunications assets.

[1] The *Telecommunications and Other Legislation Amendment Act 2017,* also known as the 'Telecommunications Sector Security Reform' (TSSR) introduced a regulatory framework to better manage national security risks of espionage, sabotage and foreign interference to Australia's telecommunications networks and facilities.

Critical broadcasting asset

61. The Bill introduces a definition of a ‘critical broadcasting asset’ under section 12E.

62. Broadcast media play an important role in emergencies, both in disseminating and collecting information about an incident. While there is no legislative requirement for broadcasters to undertake the role of warning communities, the Commonwealth, state and territories have established working relationships with broadcasters to ensure emergency information is disseminated to the community. However, the ability for national and commercial broadcasters to deliver emergency messages is dependent on the resilience and security of transmission and distribution infrastructure. The "Black Summer" fires across 2019-20 provided countless examples of the impact to significant population hubs when transmission infrastructure that is relevant to radio and television services is interrupted or taken down.

63. The definition aims to capture the transmission and distribution infrastructure which all national and commercial broadcasters rely on, and are operated by a small number of entities. For example, the ABC primarily relies on transmission assets operated by BAI Communications Australia, and infrastructure operated by TX Australia supports the Nine Network and the Seven Network in metropolitan regions.

64. A ‘critical broadcasting asset’ is defined as one or more broadcasting transmission assets owned and operated by the same entity and:

    - the entity operates from at least 50 different sites; or
    - the asset is located on a site that is prescribed in the rules as critical.

65. The Bill will define a ‘broadcasting transmission asset’ as:

    a. a radio communications transmitter; or

    b. a broadcasting transmission tower; or

    c. an associated transmission facility;

    that is used, or capable of being used, in connection with the transmission of a national broadcasting service, commercial radio broadcasting service, or a commercial television broadcasting service.

66. Limiting the application of the threshold to 50 or more sites ensures that smaller operators are unaffected by the reforms. Home Affairs understands that this definition will capture six entities: BAI Communications, Win/Prime, Seven West Media, Grant Broadcasters, TX Australia and Imparja Australia.

67. Through consultation with the ACMA, Department of Infrastructure, Transport, Regional Development and Communications, and industry, Home Affairs understands that in some regional or rural areas, communities may be reliant on a single transmission site. These critical sites will be able to be captured through the power to prescribe specific sites in the rules should it be determined that this is required for the purposes of the Act.

Responsible entity

68. For ‘critical broadcasting assets’, the responsible entity will be the owner or operator of the asset; or, if applicable, another entity that is prescribed by the rules in relation to the asset. This is appropriate as that will be the entity best placed to manage the day-to-day operations of the asset and therefore ensure security and resilience of the asset in line with this regime.

Critical domain name system

69. A 'critical domain name system' will be defined as a system that is owned by an entity that is the subject of a determination under subsection 474(1) of the *Telecommunications Act 1997* and is used to administer an Australian domain name system.

70. The .au namespace plays an important role in supporting the digital economy with over 3.2 million domain names registered as at August 2020. With the online environment becoming increasingly enmeshed with everyday life, a disruption to a critical Domain Name System (DNS) could have significant implications for Australian businesses, government and the community. Failure of the DNS could result in a loss of internet access as experienced by Telstra customers in Victoria, New South Wales, the Australian Capital Territory and Tasmania in August 2020. Malicious or criminal exploitation of the DNS can compromise users' ability to conduct business, navigate the internet or their data.

Responsible entity

71. For a 'critical domain name system', the responsible entity will be the ***declared manager of electronic addressing*** that is the subject of a determination under subsection 474(1) of the *Telecommunications Act 1997*; or, if applicable, another entity that is prescribed by the rules in relation to the asset. This is appropriate as that will be the entity best placed to manage the day-to-day operations of the asset, and therefore ensure security and resilience of the asset in line with this regime.

72. The Australian Government has reserve powers in relation to the .au namespace and the inclusion of this asset will reinforce the existing framework. Currently, the Government has endorsed .au Domain Administration Ltd (auDA) to administer the .au namespace in the public interest and perform the following core functions, among others:

    - ensure stable, secure and reliable operation of the .au domain space; and
    - respond quickly to matters that compromise DNS security.

73. Home Affairs recognises that ICANN has authority over the global technical coordination to ensure that the Internet domain name system continues to provide an effective and interoperable global naming system. The ICANN Sponsorship Agreement sets out the technical responsibilities and obligations of ICANN and auDA in managing the .au namespace.

74. In recognition of the current governance and oversight mechanisms, it is proposed that the Positive Security Obligation will remain dormant for this subsector. Should there be an identified need to activate the Positive Security Obligation, the proposed measures will take into account the existing arrangements with the Australian Government's Terms of Endorsement and the ICANN Sponsorship Agreement.

Regulator

75. Currently, the Department of Home Affairs regulates TSSR and this arrangement will remain in place. We continue to engage with relevant stakeholders in relation to the most appropriate regulator for the communications sector.

DATA STORAGE OR PROCESSING

<u>Sector definition</u>

76. The Bill introduces a definition of the 'data storage or processing sector'. The 'data storage and processing sector' is defined as the sector of the Australian economy that involves providing data

storage or processing services on a commercial basis. Entities that fall within the sector definition will be covered by the government assistance measures.

77. The sector definition aims to reflect the assets that are critical to maintaining the commercial supply and availability of data and cloud services located in Australia. This includes enterprise data centres, managed services data centres, colocation data centres and cloud data centres. The sector definition also includes the three types of cloud services: infrastructure as a service (IaaS), software as a service (SaaS) and platform as a service (PaaS).

78. New high-speed networks are enabling an exponential growth in services including the Internet of Things and cloud technology. In 2019, Deloitte reported that the adoption of cloud services by businesses in Australia has resulted in a cumulative productivity benefit to the economy of $9.4 billion over the previous 5 years, with 42per cent of businesses in Australia using a paid cloud.

79. Industries that have the highest adoption rates of cloud services include information, media and telecommunications (64per cent of businesses in the industry), mining (53 per cent), healthcare and social assistance (45 per cent) and retail trade (42 per cent).[2]

80. While the adoption of data storage and cloud services offers numerous economic and social benefits, it also introduces new risks for data security as businesses and governments aim to address challenges such as skill shortages in IT and cybersecurity, compatibility of new technologies with legacy systems and the cost associated with maintaining IT infrastructure. More than ever, commercially sensitive and personal data is being uploaded and processed online. This presents an attractive target for malicious actors.

81. As companies rely on third party providers for data storage and processing services for operational needs, these services have become vital for business continuity. It is expected that as demand for cloud services increases, there will also be an increase for data storage services, including Disaster Recovery as a Service to address the risk of data centre outages. In recognising this aspect, it is important that in the rare instances where these entities are unable to address specific hazards independently or adequately, the Government will be able to exercise its powers under the Act to support mitigation and recovery efforts.

<u>Critical infrastructure asset definition</u>

Critical data storage or processing asset

82. The Bill introduces a definition for ‘critical data storage or processing asset’ under section 12F. Assets that fall within this definition may be subject to each of the Positive Security Obligation:

    - The requirement to adopt and maintain a risk management program (Part 2A), in the event that the asset is specified in the rules under section 30AB to require such a program for this class of assets.

    - Mandatory reporting of serious cyber security incidents, in the event that the asset is specified in the rules under section 30BB to require this for this class of assets.

    - Providing of ownership and operator information, in the event that the asset is specified in the rules under section 18A to require this for this class of assets.

83. The responsible entity for each of the assets (outlined below) is the entity that will be required to comply with each of the above obligations, if turned on.

[2] Deloitte Access Economics (2019), *The economic value of cloud services in Australia*

84. An asset is a ‘critical data storage or processing asset’ if it is owned or operated by an entity that is a data storage or processing provider; and:

    a. it is used wholly or primarily in connection with a data storage or processing service that is provided on a commercial basis to an end-user that is:

        i. the Commonwealth, a State or a Territory; or

        ii. a body corporate established by a law of the Commonwealth, a State or a Territory; or

    b. it is used wholly or primarily in connection with a data storage or processing service that is provided on a commercial basis to an end-user that is:

        i. the responsible entity for a critical infrastructure asset; and

        ii. relates to business critical data; and

    c. the provider knows that the ‘critical data storage or processing asset’ is used as described in paragraphs a. and b.

85. This definition aims to capture the physical infrastructure or computing platforms used primarily for storing or processing data on a commercial basis, where the entity knows that it is a direct supplier to specified entities. The definition covers data centres and cloud service providers that manage data of significance to Australia’s national interest. It is not intended to cover instances where data storage is secondary to, or simply a by-product of, the primary service being offered, for example, accounting services that may result in the storage of some of their client’s data.

86. ‘Business critical data’ will be defined in the Bill as:

    a. personal information (within the meaning of the Privacy Act 1988) that relates to at least 20,000 individuals; or

    b. sensitive information (within the meaning of Privacy Act 1988); or

    c. information relating to any research and development in relation to a critical infrastructure asset; or

    d. information relating to any systems needed to operate a critical infrastructure asset; or

    e. information relating to risk management and business continuity (however described) in relation to a critical infrastructure asset.

87. These amendments align with the existing data reporting requirements under section 5 of the SOCI Rules. The definition of business critical data is intended to capture information that is crucial to the operation and maintenance of the critical infrastructure asset, and where any compromise to the integrity, availability or confidentiality of that information would affect the availability or reliability of the critical infrastructure asset itself or have national security implications.

88. Business critical data also includes personal data that relates to at least 20,000 individuals or sensitive information (as defined in the *Privacy Act 1988*). This seeks to protect individual privacy and promote public trust in services provided by Government and critical infrastructure assets and encourage widespread take-up of those services.

Responsible entity

89. For a 'critical data storage or processing asset' the responsible entity is the entity that is a data storage or processing provider to the end-user identified in proposed section 12F, namely users that are Commonwealth, State or Territory Government clients and other critical infrastructure assets. This is appropriate as that will be the entity best placed to manage the day-to-day operations of the asset and therefore ensure security and resilience of the asset in line with this regime.

90. Home Affairs understands that this threshold would capture at least 100 data centre entities, including those entities on the Digital Transformation Agency Government Supply Panel, and at least 30 cloud service providers.

Notification requirement

91. Consultation with industry has highlighted that a data storage or processing provider may not always know if they are providing services relating to business critical data of a critical infrastructure asset, and therefore they may be unable to determine whether they are captured by subsection 12F(2). For example, data privacy requirements typically mean that third party providers do not have visibility over what type of data is being stored or processed through their facilities.

92. In response to these concerns, the asset will only become a critical data storage or processing asset where the responsible entity knows that it is storing or processing business critical data of a critical infrastructure asset.

93. Subsection 12F(3) outlines a notification requirement for responsible entities of critical infrastructure assets in relation to data storage and processing. When a responsible entity becomes aware that a data storage or processing service is being provided by another entity on a commercial basis, and relates to business critical data, the responsible entity must take reasonable steps to inform their data storage or processing service provider as soon as practicable.

94. Responsible entities who fail to meet this notification requirement may attract a maximum civil penalty of 50 penalty units.

95. Commonwealth, State and Territory Governments will not be required to notify data and cloud service providers that they are critical data storage and processing assets. In these circumstances, it is expected that the relevant data or cloud service provider will already be aware that they provide services to a Government client. Nevertheless, the Department of Home Affairs will work across the Commonwealth, State and Territory governments to encourage notification as a matter of course.

DEFENCE INDUSTRY

Sector definition

96. The Bill defines the 'defence industry sector' as the sector of the Australian economy that involves the provision of critical defence capabilities. Entities that fall within the defence industry sector will be covered by the government assistance measure.

97. Defence industry supplies or produces goods, technology and services that:

    a. Defence needs to ensure ongoing access due to the highly essential nature of the good, technology or service to Defence's capability advantage; or

    b. Defence needs to limit others' access due to the highly sensitive nature of the good, technology or service and their potential impact on Defence interests.

98. The definition aims to cover entities that provide or support, whether directly or indirectly through supply chain arrangements, a critical capability which enables Defence's ability to shape Australia's strategic environment, deter actions against Australia's interests, and respond with credible military force when required to protect Australia's national security and national interests. This includes entities that supply essential goods, technologies and services to Defence to meet a critical capability need, and entities that provide critical components to such a critical capability. Many different entities may play a role in the creation and supply of a critical defence capability or asset.

Critical defence capability

99. A 'critical defence capability' includes the following: material, technology, a platform, a network, a system, and a service, that is required in connection with the defence of Australia or national security.

100. It is not possible to identify and describe all items that may be a defence critical capability, as what is critical shifts to reflect the changing risks to Australia's national security. Broadly, critical capabilities include those that provide the ability to:

    a. support operational requirements to respond to an existing or imminent threat;

    b. provide support to, prepare for, and sustain additional government-directed operations;

    c. maintain high-readiness contingency forces;

    d. conduct government directed regional engagement;

    e. maintain and sustain Defence capability for force generation, including training, medical, health and welfare; and

    f. deliver business continuity for Defence and defence industry.

<u>Critical infrastructure asset definition</u>

Critical defence industry asset

101. A 'critical defence industry asset' is an asset that is being, or will be, supplied by an entity to the Department of Defence, or the Australian Defence Force, under a contract; and consists of, or enables, a critical defence capability.

102. As outlined above, a critical Defence capability is one which provides the ability to shape Australia's strategic environment, deter actions against Australia's interests, and respond with credible military force when required to protect Australia's national security and national interests. This definition includes only those goods and services that are provided directly to Defence to meet a critical capability need, as well as critical components to those goods, technologies and services.

103. This definition is intended to exclude those industry entities that could be considered key enablers of Defence capability but would be captured under other sectors in the Bill (e.g. electricity or water).

104. The definition of critical defence industry asset is intended to be a sub-set of the 'critical military-related goods, services and technologies' identified in the context of the proposed reforms to the *Foreign Acquisitions and Takeovers Regulations 2015*; noting reforms to Australia's foreign investment review framework are still subject to Parliamentary consideration.

105. While assets that fall within this definition may be subject to each of the Positive Security Obligations, it is proposed that the Department of Defence will continue to manage security practices through its pre-existing DISP framework. However, the Government Assistance measures and the Enhanced Cyber Security Obligations (if any critical defence assets are designated as systems of national significance) will apply.

Responsible entity

106. Responsible entity has the meaning given by subsection 12L(22). A responsible entity for a critical defence industry asset is an entity that supplies, or will supply, under a contract, a critical defence industry asset to the Department of Defence or the Australian Defence Force.

107. These entities have been identified as responsible entities as they would be the authorised operators or suppliers of critical defence industry assets, and, as such, ultimately responsible for these assets. Given this, they are best placed to bear the obligations in Parts 2, 2A, and 2B of the Bill.

FINANCIAL SERVICES AND MARKETS

Sector definition

108. The Bill introduces a definition of the 'financial services and markets sector'. The financial services and markets sector definition captures entities that play a role in the integrity and functioning of the Australian financial services and markets sector, and are important to ensuring the delivery of essential banking and finance services. Entities that fall within the financial services and markets sector will be covered by the government assistance measure. This will ensure Government can provide assistance where there is a serious cyber incident that is detrimental to Australia's national interest. According to Boston Consulting Group, financial firms are 300 times more likely than other institutions to experience cyber attacks.

109. The financial services and markets sector is defined as the sector of the Australian economy that involves carrying on banking business (defined in the *Banking Act 1959*), operating a superannuation fund (defined in the *Superannuation Industry (Supervision) Act 1993*), carrying on insurance business (defined in the *Insurance Act 1973*), carrying on life insurance business (defined in the *Life Insurance Act 1995*), carrying on health insurance business (defined in the *Private Health Insurance Act 2007*), operating a financial market (defined in Chapter 7 of the *Corporations Act 2001*), operating a clearing and settlement facility (defined in in Chapter 7 of the *Corporations Act 2001*), operating a derivative trade repository (defined in Chapter 7 of the *Corporations Act 2001*), administering a financial benchmark (defined in in Part 7.5B of the *Corporations Act 2001*); operating a payment system (defined in the *Payment Systems (Regulation) Act 1998*), carrying on financial services business (defined in the *Corporations Act 2001*) or operating a credit facility business (as defined in the Australian Securities and Investments Commission Regulations 2001).

Critical infrastructure asset definition

110. Assets that fall within any of the below definitions may be subject to each of the Positive Security Obligation:

- The requirement to adopt and maintain a risk management program (Part 2A), in the event that the asset is specified in the rules under section 30AB to require such a program for this class of assets.

- Mandatory reporting of serious cyber security incidents, in the event that the asset is specified in the rules under section 30BB to require this for this class of assets.

- Providing ownership and operator information, in the event that the asset is specified in the rules under section 18A to require this for this class of assets.

111. The responsible entity for each of the assets (outlined below) is the entity that will be required to comply with each of the above obligations, if turned on.

Critical banking asset

112. The Bill introduces a definition of 'critical banking asset', recognising the role banking businesses play in the financial system, holding the majority of financial system assets. In addition to retail deposit-taking and lending activities, banks are involved in financial intermediation, including business banking, trading in financial markets, stockbroking, insurance and funds management.

113. Critical banking asset is defined as an asset that is owned or operated by an authorised deposit-taking institution (as defined in the *Banking Act 1959*) or a related body corporate of that institution (where related body corporate has the same meaning as in the Corporations Act 2001) and is critical to carrying on of banking business. The rules may prescribe specific assets that are critical to the carrying on of banking business by an authorised deposit-taking institution and requirements for such assets.

Responsible entity

114. The responsible entity for a critical banking asset is an authorised deposit-taking institution. Authorised deposit-taking institutions have been identified as responsible entities as they would be the authorised operators of critical banking assets, and, as such, ultimately responsible for these asset's continued operation. Given this, they are best placed to bear the obligations in Parts 2, 2A, and 2B.

115. A severe compromise of any of Australia's major banks has the potential for significant and lasting economic and security impacts given their high volume of retail customers. Consistent with advice from existing financial regulators, the rules will outline banking businesses that are critical to the functioning of the banking sector, and may therefore be subject to Positive Security Obligation. The rules may suggest a threshold that captures those banking entities with total assets above $50 billion total. This threshold is likely to capture around 10 entities.

Critical superannuation asset

116. The Bill introduces a definition of 'critical superannuation asset', recognising the significant role superannuation funds play in the Australian economy. Superannuation represents the largest financial asset for the majority of Australian households.

117. A critical superannuation asset is as an asset that is critical to the operation of a registrable superannuation entity. The rules may prescribe specified assets that are critical to the security and reliability of operating a registrable superannuation entity and requirements for an asset to be critical to the operation of a registrable superannuation entity and requirements for such assets. Drawing on advice from existing financial regulators and the superannuation industry, to ensure the thresholds capture those entities most critical to the security and reliability of the superannuation industry, the rules may suggest a threshold that captures those superannuation entities with total assets above $20 billion. This threshold would capture approximately 30 superannuation entities.

Responsible entity

118. The responsible entity for a critical superannuation asset is a registrable superannuation entity by APRA under the *Superannuation Industry (Supervision) Act 1993* (Cth) or any other entity

prescribed by the rules in relation to the asset. Registrable superannuation entities have been identified as responsible entities as they would be the authorised operators of critical banking assets, and, as such, ultimately responsible for these asset's continued operation. Given this, they are best placed to bear the obligations in Parts 2, 2A, and 2B.

Critical insurance asset

119. The Bill introduces a definition of 'critical insurance asset', recognising that insurers play a key role in the financial system – for example, failure in a reinsurer could affect operations across a significant number of Australian insurers and some insurers pay regular payments such as disability payments.

120. Critical insurance asset is defined as an asset that is owned or operated by an entity or by a body corporate that is a related body corporate of an entity that carries on insurance business as defined in the *Insurance Act 1973*, a life insurance business as defined in the *Life Insurance Act 1995*, or a health insurance business as defined in the *Private Health Insurance Act 2007*. For these three types of insurance assets, the rules can specify particular assets that are critical to the security and reliability of carrying the insurance business, or requirements for an asset to be considered critical to the security and reliability of carrying on insurance business. Drawing on advice from existing financial regulators the threshold to be included in the rules will capture the most critical insurance providers:

- insurance businesses that have total assets above $2 billion – likely around 15 businesses;
- private health insurance businesses that have more than $0.5 billion in total assets – likely around 10 businesses; and
- life insurance businesses with total assets above $5 billion – likely around 10 businesses.

Responsible entity

121. The responsible entity for a critical insurance asset is the entity that is authorised to carry on insurance business in Australia under Section 12 of the Insurance Act 1973 (Cth); or the entity that is registered as a life insurance business under section 21 of the Life Insurance Act 1995 (Cth); or the entity registered as a private health insurer under section 15 of the Private Health Insurance (Prudential Supervision) Act 2015 (Cth).

122. These entities have been identified as responsible entities as they would be the authorised operators of critical insurance businesses, and, as such, ultimately responsible for these assets' continued operation. Given this, they are best placed to bear the obligations in Parts 2, 2A, and 2B.

Critical financial market infrastructure asset

123. The Bill introduces a definition of 'critical financial market infrastructure asset', recognising that financial market infrastructures are key components of the financial system. They deliver services critical to the smooth functioning of financial markets and financial stability. Australian financial market infrastructures support transactions in securities with a total annual value of $18 trillion and derivatives with a total annual value of $185 trillion (figures reflect the value of securities trades and notional value of derivatives trades for the year to 31 December 2019). A significant disruption to financial market infrastructures would have a detrimental impact in terms of public trust, financial stability and market integrity and efficiency. The reasons for this include their central position within the financial system and inability of participating financial institutions and, in most cases, ultimately also consumers and businesses to leverage substitute services.

124. A critical financial market infrastructure asset is defined as any of the following assets:

- An asset that is owned or operated by the holder of an Australian market licence that is incorporated in Australia or a related body corporate of that licence holder, and is critical to the operation of a domestic financial market.
    - Consistent with advice from existing financial regulators, the rules may suggest a threshold that may capture a narrower cohort of the 11 Domestic (s795B(1)) Tier 1 market licensees, and be determined by a turnover metric.
    - Financial markets enable Australians to access debt, invest surplus moneys and protect against uncertain events in the future. Financial markets are used to raise capital, borrow and lend funds, invest in equities and debt securities, and transact in derivatives for risk management purposes. Without clearing and settlement facilities, and access to financial benchmarks, many financial markets could not operate.
- An asset that is owned or operated by the holder of an Australian clearing and settlement facility licence that is incorporated in Australia or a related body corporate of that licence holder and is critical to the operation of a clearing and settlement facility.
    - Consistent with advice from existing financial regulators, the rules may suggest a threshold that may capture key clearing and settlement facilities, and would likely cover the four ASX Group clearing and settlement facilities.
    - Without clearing and settlement facilities, and access to financial benchmarks, many financial markets could not operate. Large and systemically important clearing and settlement facilities are major providers of services to the Australian market for products that are integral to the Australian financial system, and can be highly interconnected with other parts of the financial system.
- An asset that is owned or operated by the holder of a benchmark administrator licence that is incorporated in Australia or a related body corporate of that licence holder and is critical to the administration of a financial benchmark.
    - Currently only 1 of the 5 Significant Financial Benchmarks designated in ASIC Corporations (Significant Financial Benchmarks) Instrument 2018/420 would be captured under this asset definition.
    - Financial benchmarks measure the price or performance of certain financial products or classes of financial products and are therefore critical to the smooth functioning of financial markets. Financial benchmark administrators are responsible for administering benchmarks that have been declared to be systemically important to the Australian financial system or where disruption to the benchmark would risk material financial disruption.
- An asset that is owned or operated by the holder of an Australian derivative trade repository licence that is incorporated in Australia or a related body corporate of that licence holder and is critical to the operation of a derivative trade repository.
    - The rules may outline a metric to determine a threshold for criticality. Whilst there is currently no domestically incorporated derivative trade repository that is licensed in Australia, the intention of including derivative trade repositories it to future proof the regime for the emergence of a domestic derivative trade repository.
    - Derivative trade repositories are a core component of the infrastructure supporting derivatives markets. A derivative trade repository may be part of a network linking various entities (e.g. clearing and settlement facilities, dealers or financial custodians)

and therefore a disruption in a derivative trade repository could risk spreading to linked entities.

- An asset that is critical to the operation of a critical payment system. Rules may prescribe attributes which, if present in a payment system, mean that such a payment system is critical to ensuring the security and reliability of the payment system. These attributes may include, but not be limited to:
    - a minimum aggregate value and/or volume of Australian dollar payments processed through the system over a specified period;
    - the time-criticality of the payments processed;
    - a minimum average value of the payments processed through the system over a specified period;
    - the provision of important payment services for which there are few or no close substitutes;
    - the system being used to settle payments that effect settlement in one or more financial market infrastructures; or
    - other factors indicating that the system has the potential to trigger or transmit systemic disruption, or, if unavailable, result in significant disruption to economic activity.
- Payment systems are arrangements through which individuals, businesses and government entities transfer funds between each other. The smooth functioning of payment systems can be important for economic activity and financial stability, and payment information is sensitive to both integrity and confidentiality risks.

125. The rules may prescribe specified assets that are critical to the operation of financial market infrastructure, or additional requirements for an asset to be critical to the security and reliability of financial market infrastructure.

Responsible entity

126. The responsible entity for critical financial market infrastructure assets are:

- For domestic financial markets, the entity that holds an Australian market licence within the meaning of the Corporations Act 2001.
- For Australian clearing and settlement facilities, the entity that holds an Australian clearing and settlement facility licence within the meaning of the Corporations Act 2001.
- For benchmark administrators, the entity that holds a benchmark administrator licence granted under the Corporations Act 2001.
- For, derivative trade depositories, the entity that holds an Australian derivative trade repository licence within the meaning of the Corporations Act 2001.
- For payment systems, an entity specified in the rules.

127. These entities have been identified as responsible entities as they would be the authorised operators of critical education assets, and, as such, ultimately responsible for these asset's continued operation. Given this, they are best placed to bear the obligations in Parts 2, 2A, and 2B.

Regulator

128. The financial sector has several mature Commonwealth regulators with complementary responsibilities, including the Australian Prudential Regulation Authority, the Australian Securities and Investments Commission and the Reserve Bank of Australia. As recommended by a number of submissions to the Protecting Critical Infrastructure and Systems of National Significance Consultation Paper, existing regulatory frameworks will be leveraged wherever possible to administer the regime for critical infrastructure assets in the financial services and markets sector.

FOOD AND GROCERY

Sector definition

129. The Bill introduces a definition for the food and grocery sector recognising that a reliable, secure and accessible food and grocery supply are key components for the sustainment of an active and healthy life for all who live in Australians. Entities that fall within the food and grocery sector definition will be covered by the government assistance measures.

130. The Food and Grocery Sector is the sector of the Australian economy that involves:

a. manufacturing; or

b. processing; or

c. packaging; or

d. distributing; or

e. supplying;

food or groceries on a commercial basis.

131. The definition reflects those functions that are critical to maintaining the commercial supply and availability of food and grocery in Australia. This definition seeks to capture all those entities that are integral to the supply chain of the food and grocery sector. While supermarkets are often the most visible point within a supply chain, when it comes to the purchasing and acquiring of food and groceries, there are numerous suppliers and components that are required to operate successfully in order for food and groceries to make it onto the shelves of supermarkets. However, this definition is not intended to capture farming.

Critical infrastructure asset definition

Critical food and grocery asset

132. The Bill introduces a definition of a critical food and grocery asset recognising the role that these assets play in delivering essential supplies that maintain and sustain life. Assets that fall within the below definition may be subject to each of the Positive Security Obligation:

- The requirement to adopt and maintain a risk management program (Part 2A), in the event that the asset is specified in the rules under section 30AB to require such a program for this class of assets.

- Mandatory reporting of serious cyber security incidents, in the event that the asset is specified in the rules under section 30BB to require this for this class of assets.

- Providing of ownership and operator information, in the event that the asset is specified in the rules under section 18A to require this for this class of assets.

133. The responsible entity for each of the assets (outlined below) is the entity that will be required to comply with each of the above obligations, if turned on.

134. The definition of a ***critical food and grocery asset*** is a network that:

a. is used for the distribution or supply of:

i. food; or

ii. groceries; **and**

b. is owned or operated by an entity that is:

i. declared by the rules to be a critical supermarket retailer; or

ii. declared by the rules to be a critical food wholesaler; or

iii. declared by the rules to be a critical grocery wholesaler.

135. Under section 12K(2), if a food and grocery asset (also known as a network) is used for the distribution of food or groceries and that asset is operated under a contract with an entity prescribed within the rules to be a critical supermarket retailer, critical food wholesaler or critical grocery wholesaler then that asset is still taken to be operated by the critical retailer or wholesaler as prescribed by the rules. In practice, this means that if a supermarket (as prescribed within the rules) were to subcontract out the trucking of groceries from a warehouse to a supermarket, then the trucking portion of the food and grocery network would still be considered a critical food and grocery asset, even though it would not be directly operated by a critical retailer or wholesaler as prescribed by the rules.

136. This approach will capture the distribution and supply operations of critical supermarkets and wholesalers that are relevant to ensuring the availability of food and grocery. It is intended for critical supermarkets and wholesalers to be listed in rules to ensure amendments can be made to accommodate future changes to business names or any other more significant market change.

137. The COVID-19 pandemic has placed food and grocery distribution and supply under significant pressure. In particular, the last six months has highlighted how disruptions to distribution networks and other key operations of Australia's major supermarkets can seriously impact the availability of critical food and grocery to the community.

138. The supermarkets and wholesaler that are intended to be prescribed in the rules have a collective market share in excess of 80 per cent, and service regional towns and metropolitan cities. The majority of this market share sits with the Woolworths Group (approximately 32 per cent), Coles Group (approximately 27 per cent), and Aldi (approximately 12 per cent). While Costco Australia only has 12 stores in Australia, their market share has risen considerably over the last two years and their stores service large population hubs.

139. Metcash is a wholesale distributor that supplies Independent Grocers of Australia supermarkets which has an approximate market share of 7 per cent, as well as other smaller supermarket brands such as Foodland, Australian United Retailer Limited (FoodWorks), Outback Stores (in the Northern Territory, Western Australia and South Australia), Friendly Grocer and Lucky 7.

140. Other parts of the sector (for example food manufacturing) are not considered critical food and grocery assets as they are often disaggregated and, if disrupted, are unlikely to have a severe and widespread impact on the availability of food and grocery.

Responsible entity

141. The responsible entity of a ***critical food and grocery asset*** is the owner or operator of an entity:

    a. declared by the rules to be a critical supermarket retailer; or

    b. declared by the rules to be a critical food wholesaler; or

    c. declared by the rules to be a critical grocery wholesaler.

142. Another responsible entity may also be prescribed by the rules if operated in relation to a critical food and grocery asset. This inclusion has been made to provide flexibility in the assignment of who a responsible entity is, acknowledging the agility and adaptability of the food and grocery supply chain and the potential need to introduce further responsible entities in the future.

143. These entities have been identified as responsible entities as they would be the authorised operators of critical food and grocery assets, and, as such, ultimately responsible for these asset's continued operation. Given this, they are best placed to bear the obligations in Parts 2, 2A, and 2B.

Regulator

144. If no other appropriate regulator is identified, the Department of Home Affairs will regulate compliance with the Positive Security Obligation.

HIGHER EDUCATION AND RESEARCH

Sector definition

145. The Bill introduces a definition of the 'higher education and research sector'. It is defined as the sector of the economy that involves being a higher education provider as defined in the *Tertiary Education Quality and Standards Agency Act 2011*, or undertaking a research program that has received investment, funding or a grant from the Commonwealth, or is relevant to one or more critical infrastructure sectors. This definition captures institutions that contribute significantly to the Australian economy, competitiveness, skilled workforce, and Australia's global standing, both as quality providers of education and as cutting-edge research institutions. For example, this could include institutions that carry out medical research or institutions that own large-scale infrastructure that is essential to Australia's national interest.

146. Entities that fall within this sector definition will be covered by the government assistance measures.

147. The sector definition captures 178 higher education providers that are registered with the Tertiary Education and Quality and Standards Agency. This includes tertiary education institutions (such as universities) and other such higher education institutions. Early learning centres, primary and secondary schools, and other such education institutions are not captured by this definition.

148. While higher education providers account for a large portion of research activities in Australia, the Department of Home Affairs acknowledges that private institutions may also conduct nationally significant research and development. As reflected in the definition, the Department of Home Affairs has determined that nationally significant research and development are likely to have received financial assistance from the Australian Government, or relate to another critical infrastructure sector, and are therefore included in the sector definition.

149. For example, the sector definition seeks to capture those entities that have received financial assistance from the Australian Research Council or the National Health and Medical Research Council, and research activities that are relevant to the space or health sector. This ensures that private research institutions can be prescribed as critical infrastructure assets should the legislative test be met in the future.

Critical infrastructure asset definition

Critical education asset

150. The Bill introduces a definition of 'critical education asset', recognising that Australian universities contribute strongly to Australia's economy. For example, a 2018 report by London Economics found that Group of Eight universities, which comprise Australia's leading research-intensive universities, had an annual economic impact to the Australian economy of some $66.4 billion each year. Universities are also responsible for a significant portion of critical research and innovation activities in Australia. Universities Australia estimates that Australian universities undertook 34 per cent of Australia's total research and development, and more than 70 per cent of public sector research in 2017-18. Australian universities are likely to continue to be a key contributor to research and innovation activities as they are required to undertake research, and offer Masters and Doctoral research degrees, in at least three broad fields, as a condition of registration with the Tertiary Education Quality and Standards Agency. Accordingly, maintaining the security and stability of Australian universities is key to critical research and development activities, and continued prosperity in Australia.

151. A critical education asset will be defined as an institution that is owned or operated by an entity that is registered in the Australian university category of the National Register of Higher Education Providers. Assets that are critical education assets may be subject to the requirement to:

- Adopt and maintain a risk management program (Part 2A), in the event that the asset is specified in the rules under section 30AB to require such a program for this class of assets.
- Mandatory reporting of serious cyber security incidents, in the event that the asset is specified in the rules under section 30BB to require this for this class of assets.
- Providing ownership and operator information, in the event that the asset is specified in the rules under section 18A to require this for this class of assets.

152. The responsible entity for each of the assets (outlined below) is the entity that will be required to comply with each of the above obligations, if turned on.

153. The proposed critical education asset definition will capture all 40 Australian universities. Foreign universities operating in Australia are not captured by this definition. The definition for critical education asset, by referring to an institution that is owned or operated by an Australian university, would place the Positive Security Obligation on entire universities, rather than particular assets owned by a university. This allows for a consideration of the complex, multi-layered and multi-functional nature of universities. It will afford universities, and industry stakeholders such as the Group of Eight and Universities Australia, the opportunity to work with the Department of Home Affairs during the co-design period to consider how, if necessary, Positive Security Obligation should apply to the various parts of the universities – including physical and electronic assets such as campuses, research labs and computing infrastructure and networks. This provides for more flexibility than if the definition were to refer to particular assets owned by universities.

154. Private research institutions have not been captured as critical infrastructure assets. Research conducted by private institutions tends to rely upon infrastructure that is already captured as critical infrastructure assets in the other sectors (such as telecommunications networks) or

Government owned facilities (such as the national research infrastructure and facilities owned or operated by the Commonwealth Scientific and Industrial Research Organisation). However, the definition of the education, research and innovation sector (outlined above) provides the ability for the Minister for Home Affairs to prescribe private research institutions as critical infrastructure assets if circumstances change in the future.

Responsible entity

155. The responsible entity for a critical education asset is a registered higher education provider that operates a critical infrastructure asset, where a registered higher education provider means an entity that is registered in the Australian university category of the National Register of Higher Education Providers.

156. These entities have been identified as responsible entities as they would be the authorised operators of critical education assets, and, as such, ultimately responsible for these asset's continued operation. Given this, they are best placed to bear the obligations in Parts 2, 2A, and 2B.

Regulator

157. Consultations with government and industry have suggested that Home Affairs may be best placed to regulate compliance with any Positive Security Obligation for the education and research sector. If determined necessary, the Department of Home Affairs will work with government and industry stakeholders to develop sector-specific Positive Security Obligation and associated guidance.

HEALTH CARE AND MEDICAL SECTOR

Sector definition

158. The Bill introduces a definition of the 'health care and medical sector'. It is defined as the sector of the Australian economy that involves the provision of health care, or the production, distribution or supply of medical supplies. Entities that fall within this sector will be covered by the government assistance measure.

159. Evidence suggests that cyber security incidences are a significant area of concern for the health care and medical sector. According to the Office of the Australian Information Commissioner, the health sector has remained among the top reporting sectors for data breaches since January 2018. In 2019, the Victorian health sector was subject to a ransomware attack, and Advanced Persistent Threats targeted Australian health sector organisations and medical research facilities during the COVID-19 pandemic.

160. International experience also highlights the dire consequences that could occur as a result of a cyber security incident. In 2017, WannaCry ransomware infected over 300,000 computers and impacted organisations in 150 countries. Among them, several health organisations were affected such as the UK National Health Service which had to cancel surgeries and divert ambulances. More recently, in September 2020, hackers disabled computer systems at Düsseldorf University Hospital in Germany, which led to the death of a patient.

161. The sector definition intends to capture those physical, electronic and other assets that are involved in the provision of health care services such as public health and preventive services, primary health care, emergency health services, hospital-based treatment, e-health services, pharmaceutical services, rehabilitation and palliative care, and diagnostic and imaging services.

162. The definition also seeks to capture those assets involved in the production of medical supplies and devices which includes products that support the provision of health care services (such as

personal protective equipment, and diagnostic equipment), pharmaceutical products and medicines, pacemakers and prosthetics. The current capture of manufacturers of medical devices is a result of the outcomes of consultation.

163. It is not intended for this definition to capture the provision of cosmetic health services or any other service that would not be recognised to be an essential function in the health sector.

164. Importantly, the definition of the sector has been developed to be intentionally broad in order to capture assets that are developed and become critical to the sector in the future. Section 9(2) also provides the Minister for Home Affairs with the ability to prescribe other parts of the sector as critical infrastructure assets within the rules should circumstances change in the future and the legislative test has been met.

Critical infrastructure asset definition

Critical Hospital

165. A *critical hospital* will be defined as a *hospital* that has a general intensive care unit. *Hospital* will have the same meaning as the *Private Health Insurance Act 2007*. This threshold is likely to capture up to 195 hospitals in metropolitan and key regional areas. This has been determined on the basis that those hospitals with intensive care units have the ability to provide specialised treatment to patients who are acutely unwell and require critical care. These hospitals have multi-disciplinary medical professionals and the necessary equipment to provide critical care for patients with a variety of medical, surgical and trauma conditions. These hospitals are therefore integral to the sustainment of life.

166. Assets that fall within the definition of a critical hospital may be subject to the requirement to:

- Adopt and maintain a risk management program (Part 2A), in the event that the asset is specified in the rules under section 30AB to require such a program for this class of assets.
- Mandatory reporting of serious cyber security incidents, in the event that the asset is specified in the rules under section 30BB to require this for this class of assets.
- Providing ownership and operator information, in the event that the asset is specified in the rules under section 18A to require this for this class of assets.

167. The responsible entity for each of the assets (outlined below) is the entity that will be required to comply with each of the above obligations, if turned on.

168. Digital infrastructure has not been captured as the Government has robust safeguards implemented around control and access defined within legislation such as the *My Health Records Act 2012*. The Government is responsible for a large portion of the digital infrastructure that supports the health sector. In particular, the Government administers the My Health Records system, which is a central records system that allows doctors, hospitals and certain other healthcare providers (such as physiotherapists) to access an individual's health records.

Responsible Entity

169. The responsible entity for a critical hospital is:

a. if the critical hospital is a public hospital—the local hospital network that operates the hospital; or

b. if the critical hospital is a private hospital—the entity that holds the licence, approval or authorisation (however described), under a law of a State or a Territory to operate the hospital; or

c. if another entity is prescribed by the rules in relation to the hospital—that other entity.

170. These entities have been identified as responsible entities as they would be the authorised operator of the critical hospital and, as such, ultimately responsible for the hospital's continued operation. This is appropriate as that will be the entity best placed to manage the day-to-day operations of the asset and therefore ensure security and resilience of the asset in line with this regime.

Regulator

171. The Department of Home Affairs will regulate compliance for the Positive Security Obligation.

TRANSPORT

Sector definition

172. The Bill introduces a definition of the transport sector defining it as the sector of the Australian economy that involves owning or operating assets that are used in connection with the transport of goods or passengers on a commercial basis; or the transport of goods or passengers on a commercial basis. Entities that fall within the sector definition will be covered by the government assistance measures.

173. This recognises the role that these assets play in maintaining the commercial supply and availability of transport services in Australia to facilitate the important and export of goods. The geographic spread of Australia's population coupled with economic reliance on goods that are produced in remote areas means that national commerce and living standards relies on the reliable and efficient transport of goods and passengers across regions.

174. The definition extends beyond the primary service of providing transport for goods or passengers on a commercial basis, to entities that own or operate assets used in connection with that service. The definition is intended to capture the first link of the supply chain that enables the transport sector to function, recognising that disruption to those underlying assets can undermine the operation of Australia's transport sector in a manner that damages Australia's economic activity and national security. For instance, the transport of essential food and groceries into remote areas of the Northern Territory relies on the availability of long combination vehicles or 'road trains' as they are commonly referred to in Australia.

Critical infrastructure asset definition

175. Assets that fall within each of the below critical infrastructure asset definitions for this sector may be subject to the requirement to:

- The requirement to adopt and maintain a risk management program (Part 2A), in the event that the asset is specified in the rules under section 30AB to require such a program for this class of assets.

- Mandatory reporting of serious cyber security incidents, in the event that the asset is specified in the rules under section 30BB to require this for this class of assets.

- Providing ownership and operator information, in the event that the asset is specified in the rules under section 18A to require this for this class of assets.

176. The responsible entity for each of the assets (outlined below) is the entity that will be required to comply with each of the above obligations, if turned on.

Critical assets in the aviation and maritime sectors

177. Currently, section 11 of the SOCI Act lists 20 maritime ports as a 'critical port.' This definition will remain unchanged. The Bill will also introduce a new definition of 'critical aviation asset'. The definition will cover assets owned and operated by an aircraft operator or a regulated air cargo agent where those assets are used in connection with the provision of an air service. It will also include assets owned and operated by an airport operator where those assets are used in connection with the operation of an airport.

178. For the positive security obligations to apply to a 'critical port' or 'critical aviation asset' a rule must be made by the Minister for Home Affairs to turn the obligations on. The aviation and maritime sectors already have robust security frameworks in place, in the *Aviation Transport Security Act 2004* and the *Maritime Transport and Offshore Facilities Security Act 2003*. Comprehensive reforms to these regimes will be progressed in early 2021. This will ensure that key assets regulated by these regimes would similarly implement the positive security obligation, including in relation to the significant threat posed by cyber and systems attacks.

179. As such, there is no intention to apply the SOCI Act positive security obligations to the aviation or maritime sectors at this point in time. This will allow sufficient time to amend both the *Aviation Transport Security Act 2004* and the *Maritime Transport and Offshore Facilities Security Act 2003* and will avoid duplication of regulatory requirements on industry. However, retaining the definition of 'critical port' and including a definition of 'critical aviation asset' at this stage will clarify the maritime and aviation assets on which there must be a relevant impact to trigger the powers in Part 3A—Responding to serious cyber security incidents.

180. The Department will work closely with industry to coordinate the implementation of these reforms across the aviation and maritime sectors.

Critical freight infrastructure asset – road and rail corridors and intermodal transfer facilities

181. Section 12B of the Bill defines a critical freight infrastructure asset as a road network, rail network or intermodal transfer facility that functions as a critical corridor for the transportation of goods between 2 States, a state or territory, 2 territories, or two cities or towns with populations of 10,000 or more.

182. Subsection 12B(2) enables the Minister for Home Affairs to prescribe specific road networks, rail networks or intermodal transfer facilities as critical freight infrastructure assets. When developing these rules the Department of Home Affairs will work closely with the freight industry and State and Territory Governments to identify critical segments of the road and rail sectors, where Australians' access to basic food and groceries, health services and ability to undertake economic activities will be severely affected if those segments were rendered unavailable. To identify the critical aspects of the road and rail sectors, the Department of Home Affairs will consider whether that road or rail network or intermodal transfer facility carries high volumes of freight, high value commodities, there is a high frequency of heavy vehicles, it carries specific commodities of high economic significance for the region, or whether there are alternative transport routes available if that road or rail network or intermodal transfer facility was unavailable.

183. The definition of critical freight infrastructure asset recognises the role that these assets play in ensuring capital cities and population centres separated by vast distances can access critical products (such as medical supplies and food and grocery) and the facilitating businesses that transport goods to ports and airports.

184. Such infrastructure maintains the stability and security of key road and rail infrastructure and is critical to Australia's prosperity and international competitiveness. The 2019-2020 bushfire season has also highlighted the vital role of the road and rail subsectors in responding to and

mitigating the impact of natural disasters. In addition, these are particularly significant to Australia's national interest if there is a lack of redundancy. For example, the 2009 floods in Queensland's north and north-west temporarily closed the Bruce Highway and limited the availability of food and supplies to the region.

185. Similarly, intermodal terminals play a significant role in facilitating the consolidation, storage and transfer of freight between rail and road at the beginning and end of each rail journey. Intermodal terminals provide connectivity to ports, regional networks and other capital cities and regional centres and are central to the stability and security of road and rail infrastructure.

Responsible entity

186. Subsection 12L(18) states that for critical freight infrastructure assets, the responsible entity is defined to mean a Commonwealth, State or Territory, or statutory authority established under a Commonwealth, State or Territory law, that is responsible for the management of the critical freight asset. This recognises that Australia's key road and rail networks are operated by Commonwealth, State or Territory Governments either directly or through a statutory body. In the event that these assets are no longer publically operated, the Minister for Home Affairs may prescribe the specific responsible entity for that critical freight infrastructure asset in the rules.

187. These entities have been identified as responsible entities as they would be the authorised operator of the asset and, as such, ultimately responsible for the asset's continued operation. Notably, this definition is intended to capture the responsible entity that is responsible for the care, control or management of the critical freight infrastructure asset. This can include: planning, designing, building and maintaining the critical freight infrastructure asset and delivering regulatory services to promote customer safety. Given this, they are best placed to bear the obligations in Parts 2A and 2B, alongside their register obligations in existing Part 2 of the Act.

Critical freight services asset

188. Section 12C of the Bill defines a critical freight services asset as a network used by an entity carrying on a business that is critical to the transportation of goods by road, rail, inland waters or sea. Subsection 12C(2) states that specific businesses that are critical to the transportation of goods by road or rail, or both; or requirements for a business to be critical to the transportation of goods by road or rail, or both may be prescribed in the rules.

189. This definition recognises the role that these assets play in maintaining Australia's economic prosperity and security. Critical freight services assets are critical to Australia's trade and commerce, and social stability as they are responsible for logistics and movement of valuable goods and products across the country. These entities are responsible for assisting businesses to transport products to consumers, and ensuring communities can access critical supplies, including food and grocery. For example, it is estimated that rail in Australia contributes over $26 billion to the national economy. The COVID-19 pandemic and recent natural disasters have highlighted the importance of freight entities who transported personal protective equipment, medical supplies, food and grocery, and other critical supplies across Australia.

190. When developing these rules the Department of Home Affairs will work closely with the freight industry and State and Territory Governments to identify critical freight services, where Australians' access to basic food and groceries, health services and ability to undertake economic activities will be severely affected if those services were rendered unavailable. The Department will take into account the relevant business' market share (likely based on revenue), volume and value of goods transported, whether the business is responsible for the transport of niche goods that enable the delivery of critical services (for instance medical supplies that enable intensive care units to remain operational), and whether any redundancies exist if that freight service is rendered unavailable.

Responsible entity

191. For critical freight service assets, the responsible entity is the operator of the critical freight services asset, or any other responsible entity prescribed in the rules.

192. These entities have been identified as responsible entities as they would be the authorised operator of the asset and, as such, ultimately responsible for the asset's continued operation. Given this, they are best placed to bear the obligations in Part 2A and 2B, alongside their register obligations in existing Part 2 of the Act.

Critical public transport asset

193. Section 5 of the Bill defines a critical public transport asset as a public transport network or system that is managed by a single entity and is capable of handling at least 5 million passenger journeys per month.

194. This definition recognises the role that these assets play in enhancing economic productivity and the national economy by facilitating the efficient movement of people around Australia's cities. Australia's cities are growing rapidly and are increasingly important to our prosperity. In our five largest cities (Adelaide, Brisbane, Melbourne, Perth and Sydney), close to half of the population live in the outer suburbs and have a high reliance on functioning and regular public transport networks.

195. There is clear evidence internationally that large and connected public transport networks are prime targets for terrorist activities or other unlawful acts. This is particularly due to large numbers of people being concentrated together at peak and predictable times, and the relative reliance on transporting goods or materials on the network that could potentially cause widespread damage. Some public transport providers also hold large data sets relating to their customers; including billing information and their public transport usage, which also need to be appropriately protected.

196. Narrowing the public transport asset threshold to services capable of handling at least five million passenger journeys a month recognises that critical public transport relates to the networks that service major population hubs, amplifying the significant economic impact and social disconnection caused by a disruption to those services. Consistent with advice from state and territory counterparts, this threshold has been designed to capture those Australian markets with the largest transport networks that are managed by a single entity, noting those networks have a greater capacity to absorb the regulatory impost of the reforms.

Responsible entity

197. For critical public transport assets, the responsible entity is the single entity managing the critical public transport asset or any other responsible entity prescribed in the rules.

198. These entities have been identified as responsible entities as they would be the authorised operator of the asset and, as such, ultimately responsible for the asset's continued operation. Given this, they are best placed to bear the obligations in Part 2A and 2B, alongside their register obligations in existing Part 2 of the Act.

ENERGY

<u>Sector definition</u>

199. The Bill introduces a definition of the '*energy sector*'. It is defined as the sector of the Australian economy that involves:

- the production, distribution or supply of electricity; or

- the production, processing, distribution or supply of gas; or
- the production, processing, distribution or supply of liquid fuel.

200. Entities that fall within the sector definition will be covered by the government assistance measures. This will ensure Government can provide assistance where there is a serious cyber incident that is detrimental to Australia's national interest. For instance, in the event the control systems of numerous electricity generators that individually are under the designated generation threshold outlined in the rules are attacked, it is intended that Government assistance would be available to step in to assist.

201. This definition reflects those functions that are critical to maintaining the ongoing availability of energy, essential to maintaining Australia's security and economy. For example, this includes electricity generators, gas and electricity transmission and distribution networks, gas processing and storage assets, liquid fuel refineries, transmission and storage assets and energy market operators. It does not intend to capture energy consumers.

202. If the energy sector were impacted by a significant disruption it would lead to cascading consequences for a range of other sectors, significantly impacting Australia's security and economy. The Australian energy sector provides essential services to almost all people and businesses across the Australian economy. The definition is intended to be flexible so that it continues to be relevant as business models and technologies for the supply of electricity, gas and liquid fuels change over time.

Critical infrastructure asset definition

203. Assets that fall within any of the below definitions may be subject to each of the Positive Security Obligation:

- The requirement to adopt and maintain a risk management program (Part 2A), in the event that the asset is specified in the rules under section 30AB to require such a program for this class of assets.
- Mandatory reporting of serious cyber security incidents, in the event that the asset is specified in the rules under section 30BB to require this for this class of assets.
- Providing ownership and operator information, in the event that the asset is specified in the rules under section 18A to require this for this class of assets.

204. The responsible entity for each of the assets (outlined below) is the entity that will be required to comply with each of the above obligations, if turned on.

Critical electricity asset

205. The Bill will draw on the existing definition in the SOCI Act and may extend the application to a broader set of assets, particularly generation assets. This recognises the role that these critical electricity assets play in delivering essential services to maintaining Australia's security and economy. Electricity is fundamental to every facet of Australian society, underpinning just about everything in the digital age. A prolonged disruption to Australia's electricity networks would have a significant impact on communities, businesses and national security capabilities. Some electricity providers also hold large data sets about customers and their electricity usage, which need to be appropriately protected.

206. The definition is:

- an electricity generation asset that is critical to ensuring the security and reliability of electricity networks or electricity systems in a state or territory

- an asset that is a network, system, or interconnector, for the transmission or distribution of electricity to ultimately service at least 100,000 customers. The rules may also prescribe other customer numbers as the relevant threshold.

207. Transmission, distribution and generation assets are all considered critical components of the electricity network. For example, if there was a failure or disruption in a transmission network it could lead to widespread blackouts impacting people over a large area, both within and potentially across states.

208. The rules will continue to be used to set out the requirements for an electricity generator to be considered critical to ensuring the security and reliability of electricity networks. It is likely that an expanded set of generator assets will be captured, building on the existing approach in the rules. The Department will work with industry participants to identify appropriate thresholds having regard to generation capacity, system restart functions, and other issues that may impact on system reliability or security.

Responsible entity

209. The responsible entity for a critical electricity asset will continue to be defined as the entity that holds the licence, approval or authorisation (however described), under a law of the Commonwealth, a State or a Territory to provide the service to be delivered by the asset – or, where another entity is prescribed by the rules in relation to the asset, that other entity.

210. These entities have been identified as responsible entities as they would be the authorised operator of the critical electricity asset and, as such, ultimately responsible for the electricity asset's continued operation. Given this, they are best placed to bear the obligations in Part 2A and 2B, alongside their register obligations in existing Part 2 of the Act.

Critical gas asset

211. The Bill will draw on the existing definition in the SOCI Act and may extend the application to a broader set of assets, ensuring that assets covered under this definition adopt an 'all hazards' approach to their security functions, including in relation to the significant threat posed by cyber and systems attacks. These amendments recognise that a prolonged disruption to Australia's gas networks would have a significant impact on communities, businesses and national security capabilities.

212. The definition is:

- a gas processing facility that has a capacity of at least 300 terajoules per day or any other capacity prescribed by the rules; or

- a gas storage facility that has a maximum daily withdrawal capacity of at least 75 terajoules per day or any other quantity prescribed by the rules; or

- 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 subsection (2).

213. These definitions remain the same, in principle, as under the current definitions of critical gas asset within the SOCI Act. Minor amendments have been made to clarify the thresholds upon advice from industry and Government stakeholders.

214. Assets that fall within the definition of a critical gas asset may be subject to the requirement to:

- Adopt and maintain a risk management program (Part 2A), in the event that the asset is specified in the rules under section 30AB to require such a program for this class of assets.

- Mandatory reporting of serious cyber security incidents, in the event that the asset is specified in the rules under section 30BB to require this for this class of assets.

- Providing ownership and operator information, in the event that the asset is specified in the rules under section 18A to require this for this class of assets.

215. In practice the definitions will capture gas processing facilities, storage facilities and distribution and transmission networks over a certain threshold. These assets are critical to the adequate supply of gas to end consumers for a wide range of industrial, commercial and residential uses. Gas is particularly important for gas powered electricity generators which account for approximately 20 per cent of Australia's electricity. Gas is also an important export commodity. These definitions will not cover gas retailers or gas extraction assets.

216. For a gas storage facility, amendments to the SOCI Act would clarify that the thresholds of at least 75 terajoules per day applies to the withdrawal (export) capacity of the gas storage asset. Currently, the definition of a critical gas storage asset is "a gas storage facility is a critical gas asset if it has a maximum daily quantity of at least 75 terajoules per day". This had the potential to cause confusion where an asset had different intake (import) and withdrawal (export) capacities. For clarity, the definition would be altered to read "a maximum daily withdrawal capacity of at least 75 terajoules per day".

217. Gas is defined as a substance that:

- is in a gaseous state at standard temperature and pressure; and

- consists of naturally occurring hydrocarbons, or a naturally occurring mixture of hydrocarbons and non-hydrocarbons, the principal constituent of which is methane; and is suitable for consumption.

Responsible entity

The responsible entity for a critical gas asset will continue to be defined as the entity that holds the licence, approval or authorisation (however described), under a law of the Commonwealth, a State or a Territory to provide the service to be delivered by the asset – or, where another entity is prescribed by the rules in relation to the asset, that other entity.

218. These entities have been identified as responsible entities as they would be the authorised operator of the critical gas asset and, as such, ultimately responsible for the gas asset's continued operation. Given this, they are best placed to bear the obligations in Part 2A and 2B, alongside their register obligations in existing Part 2 of the Act.

Critical liquid fuel asset

219. The Bill introduces a definition of a critical liquid fuel asset recognising the role that these assets play in delivering services that are relied upon to support the Australian economy and are essential to energy security. A prolonged disruption to Australia's liquid fuel sector would have a significant impact on communities, businesses and national security capabilities.

220. The definition is:

- a liquid fuel refinery that is critical to ensuring the security and reliability of a liquid fuel market; or

- a liquid fuel transmission pipeline that is critical to ensuring the security and reliability of a liquid fuel market; or

- a liquid fuel storage facility that is critical to ensuring the security and reliability of a liquid fuel market.

221. Assets that fall within the definition of a critical liquid fuel asset may be subject to the requirement to:

- Adopt and maintain a risk management program (Part 2A), in the event that the asset is specified in the rules under section 30AB to require such a program for this class of assets.

- Mandatory reporting of serious cyber security incidents, in the event that the asset is specified in the rules under section 30BB to require this for this class of assets.

- Providing ownership and operator information, in the event that the asset is specified in the rules under section 18A to require this for this class of assets.

222. These definitions will capture liquid fuel refineries, pipelines and storage facilities. Distribution pipelines are critical for inter-city distribution and for movement from refineries and ports to terminals. The pipelines critical for these forms of distribution will be prescribed in the rules to allow flexibility to make changes as criticality and the industry evolves over time. Storage assets are critical to ensuring continued security of supply will be prescribed in the rules. It is not intended that retail assets or extraction assets will be covered.

223. A refinery is a facility that converts raw products such as crude oil into products such as petrol, diesel and jet fuel. Raw products are distilled and separated where it is processed into a useable energy source.[3] Liquid fuel includes crude oil and condensate, as well as refined products such as petrol, diesel and jet fuels, and ethanol and biodiesel.

Responsible entity

224. The responsible entity for a critical liquid fuel asset is:

- if the asset is a liquid fuel refinery – the relevant fuel industry corporation as defined by the *Liquid Fuels Emergency Act 1984* that operates the asset;

- if the asset is a liquid fuel pipeline – the operator of the pipeline;

- if the asset is a liquid fuel storage facility – the operator of the facility;

- if another entity is prescribed by the rules in relation to the asset—that other entity.

225. These entities have been identified as responsible entities as they would be the authorised operator of the critical liquid fuel asset and, as such, ultimately responsible for the liquid fuel asset's continued operation. Given this, they are best placed to bear the obligations in Parts 2A and 2B, alongside their register obligations in existing Part 2 of the Act.

Critical energy market operator asset

226. The Bill introduces a definition of a critical energy market operator asset recognising the role that these assets play in maintaining the security of supply and the efficient operation of gas and electricity systems critical to Australia. A disruption to Australia's key market operators would

[3] Liquid Fuel Security Review – Interim Report

have a significant and widespread impacts on communities, businesses and national security capabilities.

227. A critical energy market operator asset means an asset that:

- is used by the Australian Energy Market Operator Limited (AEMO); or Power and Water Corporation; or Regional Power Corporation (Horizon Power - ABN 57 955 011 697); or Electricity Networks Corporation (Western Power- ABN 18540492861); and

- is critical to ensuring the security and reliability of an energy market.

228. In this context, an energy market operator asset is an asset that is essential to the market operator undertaking its statutory functions, for example managing market trading and ensuring the security and reliability of the physical infrastructure. Although Western Power's primary function is as a transmission and distribution network operator, it has been included within the definition of a critical energy market operator as it undertakes market operator functions.

229. Electricity and gas market operators play an essential role in ensuring electricity and gas systems operate safely and reliably, and allow for the trading of energy commodities that are ultimately sold to customers. Industry strongly recommended the inclusion of market operators in the critical infrastructure regime.

Responsible entity

230. The responsible entity for a critical energy market operator asset is defined as the entity that uses the asset.

231. These entities have been identified as responsible entities as they would be the authorised operator of the critical market operators asset and, as such, ultimately responsible for the market operator asset's continued operation. Given this, they are best placed to bear the obligations in Part 2A and 2B, alongside their register obligations in existing Part 2 of the Act.

Regulator

232. There is no existing national all-hazards regulator in the energy sector. The objectives of the national electricity and gas legislation are focussed on economic outcomes, reliable and secure supplies, and consumer protections. The Department of Home Affairs will continue to engage across the sector to determine the appropriate regulator for the energy sector.

SPACE TECHNOLOGY

Sector definition

233. The Bill introduces a definition of the '*space technology sector'*. Entities that fall within the sector definition will be covered by the government assistance measures.

234. The sector will be defined as the sector of the Australian economy that involves the commercial provision of space-related services, and reflects those functions that are critical to maintaining the supply and availability of space-related services in Australia. This definition reflects those assets and functions that are critical to maintaining the commercial supply and availability of space-related services in Australia. For example, this would include those assets, functions and components enabling operation of a space service or activity, including provision of launch (comprising the assets themselves and the systems that give integrity to those assets), including:

    a. position, navigation and timing in relation to space objects;

    b. space situational awareness services;

c. space weather monitoring and forecasting;

d. communications, tracking, telemetry & control in relation to space objects;

e. remote sensing earth observations from space;

f. facilitating access to space.

235. The Trusted Information Sharing Network Space Cross-Sectoral Interest Group noted during consultation on these reforms that any regulation of the space technology sector needed to cater for the transformation of and anticipate significant and growing changes in, the space sector. For that reason the Space Technology Sector definition aligns with the National Civil Space Priority Areas for Australia to capture the evolving nature and future direction of the sector.

Critical infrastructure asset definition

Critical space technology asset

236. The space technology sector supply chain brings together a dynamic and complex blend of Government, industry, research and international owned and operated assets and functions. Some assets and functions in these supply chains (particularly those providing critical capabilities) are owned by the Commonwealth or strategic partners, who maintain stringent security obligations akin to the proposed Positive Security Obligation.

237. The Bill does not insert a specific definition of a *critical space technology asset*. Consultation with sector stakeholders have identified that at this time critical space technology sector assets are communications assets and therefore covered under the proposed definition of critical telecommunications assets. This captures carriers and carriage service providers under the TSSR with relevance to transmitting or receiving of radio communications and optical communications to and from Space.

238. Notwithstanding this, subsection 9(2) of the current SOCI Act provides for an additional asset to be prescribed if the Minister for Home Affairs is satisfied it meets certain tests. As the space sector evolves and more critical assets are identified, section 9 will provide for those assets to be prescribed under the regime.

Responsible entity

239. For ‘critical telecommunications asset’, the responsible entity is the carrier that holds the carrier licence for the telecommunications network; or an entity that is the carriage service provider within the meaning of the *Telecommunications Act 1997*. This is appropriate as that will be the entity best placed to manage the day-to-day operations of the asset and therefore ensure security and resilience of the asset in line with this regime.

240. The Department of Home Affairs acknowledges that the TSSR framework is currently under review as part of the Parliamentary Joint Committee on Intelligence and Security’s ‘Review of Part 14 of the Telecommunications Act 1997’. The outcomes of that review will inform how the Positive Security Obligation is implemented for the telecommunications sector.

241. Revised definitions for responsible entities will be included in the rules following completion of work underway within the space industry and the Commonwealth to gain clarity on criticality for the space technology sector.

Regulator

242. As outlined above for the communications sector, the Department of Home Affairs currently regulates TSSR and this arrangement will remain in place.

WATER AND SEWERAGE

Sector definition

243. The Bill introduces a definition of the '*water and sewerage sector'***.** It is defined as the sector of the Australian economy that involves operating water or sewerage systems or networks. Entities that fall within the sector definition will be covered by the government assistance measures.

244. *Water or sewerage services* is intended to capture wastewater, potable water, raw water and recycled water. This broad threshold will capture desalination plants, water utilities and bulk water providers. This is because all four elements of water and sewerage are deemed critical to the continued supply of clean and safe water for all Australians, as well as being a key component for the functioning of other critical infrastructure.

245. This definition is intentionally broad to allow Government Assistance for a broad range of assets in the water sector. The language used captures critical suppliers to the water entities already regulated under the SOCI Act. The definition also extends to other entities participating in the sector such as chemicals suppliers.

Critical infrastructure asset definition

246. Assets that fall within the below definition may be subject to each of the Positive Security Obligation to:

- adopt and maintain a risk management program (Part 2A), in the event that the asset is specified in the rules under section 30AB to require such a program for this class of assets.
- mandatory reporting of serious cyber security incidents, in the event that the asset is specified in the rules under section 30BB to require this for this class of assets.
- providing ownership and operator information, in the event that the asset is specified in the rules under section 18A to require this for this class of assets.

247. The responsible entity for each of the assets (outlined below) is the entity that will be required to comply with each of the above obligations, if turned on.

Critical water asset

248. The Bill will draw on the existing definition in the SOCI Act for the water sector and may extend the application to a broader set of assets, ensuring that assets covered under this definition adopt an 'all hazards' approach to their security functions, including in relation to the significant threat posed by cyber and systems attacks. These amendments recognise that a disruption to Australia's key market operators would have a significant and widespread impacts on communities, businesses and national security capabilities.

249. The definition is:

- One or more water or sewerage systems or networks that are managed by a single water utility; and ultimately deliver services to at least 100,000 water connections or 100,000 sewerage connections.

250. The 100,000 connections requirement captures those critical utilities, which if disrupted, would significantly impact the operations of large population hubs, significant economic interests and Government operations. This has been determined by considering:

- Large population hubs
    - The Bureau of Meteorology currently uses 100,000 connections as its highest data point to capture the water utilities servicing the major population hubs in Australia.
    - As a collective, these utilities service approximately 80 per cent of Australia's population.
- Critical infrastructure interdependencies which for water includes but is not limited to agricultural purposes, data centres, electricity generation stations, hospitals, military facilities and telecommunications infrastructure.

251. The water thresholds remain unchanged as they are still deemed suitable to achieve the objectives of the Act.

252. A threshold of 100,000 connections captures 29 water and sewerage systems or networks. The Minister for Home Affairs may choose to designate additional assets that fall below the 100,000 connection but are considered critical for electricity generation or for other purposes. It is not intended that water extraction assets or water consumers will be captured.

Responsible entity

253. A *water utility* means an entity that holds a licence, approval or authorisation (however described), under a law of the Commonwealth, a State or a Territory, to provide the service to be delivered by the asset; or if another entity is prescribed by the rules in relation to the asset—that other entity. This is largely unchanged for the existing definition in the SOCI Act.

254. These entities have been identified as responsible entities as they would be the authorised operator of the critical market operators asset and, as such, ultimately responsible for the market operator asset's continued operation. Given this, they are best placed to bear the obligations in Part 2A and 2B, alongside their register obligations in the existing Part 2 of the Act.

Regulator

255. The Department of Home Affairs will regulate compliance for the Positive Security Obligation, in line with existing arrangements for the sector under the SOCI Act Pricing and customer bills will not be the subject of the Positive Security Obligation.

PART 2 – DETAILED EXPLANATION OF PROVISIONS

256. A key component of the enhanced critical infrastructure security framework is the creation of a holistic positive security obligation for critical infrastructure assets. The positive security obligation will contain the following elements and will only apply in circumstances where the Minister for Home Affairs has made a rule turning the specific obligation on for particular critical infrastructure assets:

a. providing ownership and operator information for the Register of Critical Infrastructure Assets (in line with the existing requirement in Part 2 of the SOCI Act);

b. adopting and maintaining a critical infrastructure risk management program; and

c. mandatory reporting of cyber security incidents to the Australian Signals Directorate (ACSC).

257. An uplift in security and resilience across critical infrastructure sectors will mean that all businesses will benefit from strengthened protections to the networks, systems and services we all depend on. The regime will embed preparation, prevention and mitigation activities into the business as usual operation of critical infrastructure assets, providing certainty for businesses across all critical infrastructure sectors by setting clear security standards.

258. The regime will also provide greater situational awareness of threats to critical infrastructure assets, allowing the Government to respond effectively and efficiently to emergencies, and provide industry with access to relevant risk information, expertise and advice prepared by the ACSC. This approach will better align with business and community expectations for Government to take proportionate action when required to protect our essential services.

PART 2 – REGISTER OF CRITICAL INFRASTRUCTURE ASSETS

259. Part 2 of the current SOCI Act creates a Register of Critical Infrastructure Assets which is designed to assist the Government to gain greater visibility of who owns, controls and has access to critical infrastructure assets, including board structures, outsourcing and offshoring information, ultimately ensuring the security and resilience of critical infrastructure.

260. The Register requires reporting entities, who are either direct interest holders or the responsible entity of critical infrastructure assets, to provide interest and control information and operational information to the Secretary within a certain timeframe.

Amendments to Part 2 – Register of Critical Assets

261. The Bill makes two key changes to the Register of Critical Infrastructure Assets.

262. The first change is that, through the addition of other critical infrastructure assets into section 9 of the Act, the range of reporting entities that will be subjected to reporting obligations will increase. The increased coverage of the *Register* enables the Government to develop and maintain a comprehensive picture of the ownership and operational arrangements of critical infrastructure assets across all critical infrastructure sectors. Analysis of the information in the Register will enable the Critical Infrastructure Centre to:

- assess ultimate ownership of assets and influences by particular individuals or companies;
- analyse interdependencies among critical infrastructure assets and sectors; and

- identify commonalities in services being used by critical infrastructure assets, such as shared IT service providers or shared control systems.

263. The second change is that rules made by the Minister for Home Affairs for the purposes of section 18A will determine who is subject to the Register obligations in Part 2. This effectively works as an 'on switch' through which the Minister can ensure that this particular aspect of the positive security obligation only applies in appropriate situations. For example, the Minister may choose not to apply Part 2 to a class of critical infrastructure assets, if the information is already available to government through other means. Importantly, this will be used to avoid duplicate reporting to Government and thus reduce regulatory burden. Section 18A also provides that those assets currently covered by the Act will continue to be bound by the Register obligations, ensuring a continuity of obligations.

264. Entities will continue to have six months to comply with their reporting obligations once their obligations commence.

265. Under the current SOCI Act, non-compliance by an entity with the obligations in Part 2 relating to the provision of Register information may attract civil penalties.

266. Importantly, the Register of Critical Infrastructure Assets is not public. The information on the Register may be sensitive and could be detrimental to the commercial interests of reporting entities if the information is made public. To maintain confidentiality, the SOCI Act provides that any information provided to the Register is protected information under the Act and may only be used, recorded and disclosed in limited circumstances. Unlawful disclosure of protected information, attracts a penalty of two years imprisonment or 120 penalty units, or both.

PART 2A - CRITICAL INFRASTRUCTURE RISK MANAGEMENT PROGRAMS

267. During consultations, industry welcomed the establishment of a clear and consolidated legislative obligation to give industry a sound basis for taking a more comprehensive risk management approach. The Bill achieves this through the new requirements in Part 2A for critical infrastructure assets to develop and comply with a critical infrastructure risk management program - the second limb of the positive security obligation.

268. These amendments are intended to uplift core security practices of critical infrastructure assets by ensuring responsible entities take a holistic and proactive approach toward identifying, preventing and mitigating risks from all hazards.

269. The Bill sets out the overarching obligations for the risk management programs with the more detailed, sector-specific requirements to be contained in rules. Noting that the responsible entity is best placed to understand the risks to an asset and develop appropriate risk practices, this obligation has been designed to be principle based. Combined, the SOCI Act and the proposed rules will ultimately require responsible entities of critical infrastructure assets to manage security risks by meeting the following principles-based outcomes:

a. **Identify material risks –** Entities will have a responsibility to take an all-hazards approach when identifying risks that may affect the availability, integrity, reliability and confidentiality of their asset. This will require considering of both natural and human induced hazards which pose a material risk, with the detail to be outlined in sector specific rules to be co-designed with industry. This may include understanding how these risks might accumulate throughout the supply chain, understanding the way systems are interacting, and outlining which of these risks may have a significant consequence to core service provision.

b. **Mitigate risks to prevent incidents –** Entities will be required to understand the identified risks and have appropriate risk mitigations in place to manage those risks. Risk mitigation should consider both proactive risk management as well as having processes in place to detect and respond to threats as they are being realised to prevent the risk from eventuating.

c. **Minimise the impact of realised incidents –** Entities will be required to have robust procedures in place to mitigate the impacts in the event a threat has been realised and recover as quickly as possible. This may include ensuring plans are in place for a variety of incidents, such as having back-ups of key systems, adequate stock on hand, redundancies for key inputs, out-of-hours processes and procedures, and the ability to communicate with affected customers.

d. **Effective governance –** Through rules, entities will be required to have appropriate risk management oversight arrangements in place, including evaluation and testing. This will involve strong governance with clear lines of accountability, demonstrated comprehensive planning, and a robust assurance and review process. Compliance will be assessed by the relevant regulator noting that what is appropriate will be unique to each entity. Regulators will focus on security and resilience outcomes and seek to avoid compliance action wherever possible.

Who must comply?

270. Similar to the other limbs of the positive security obligation, section 30AB provides a mechanism through which the Minister for Home Affairs may activate the risk management obligations contained in Part 2A for particular critical infrastructure assets. This must be done through making a rule, or where a declaration under section 51 determines that this Part applies to the asset. This 'on-switch' is intended to prevent duplication where arrangements in sectors already exist which impose equivalent obligations to the risk management program. In these circumstances, the SOCI Act obligations will remain dormant with those existing obligations continuing to apply without duplication.

271. For example, the security and resilience of critical defence industry assets is currently managed through existing frameworks and obligations under the Defence Industry Security Program (DISP). The DISP is a non-regulatory risk management program run by the Department of Defence (Defence) that strengthens security practices in partnership with industry. Existing Defence security mechanisms under the DISP are considered sufficient and as such the risk management program is unlikely to be turned on for this class of assets, absent a significant change in the threat environment or in industry practices.

272. However, the Minister for Home Affairs retains the power to activate the risk management program over time should it be considered appropriate and necessary to achieving security outcomes, following consultation with the relevant Minister and industry.

273. Any rules made under section 30AB to activate the risk management program will be disallowable by Parliament.

274. Acknowledging that bringing business practices into line with these obligations may take time, and that certainty about the requirements to be provided in the rules is necessary before such investments can be made, any rules to apply Part 2A to an asset and provide the sector-specific requirements for the program will, unless exceptional circumstances exist, have a six month delayed commencement to allow an appropriate transition period.

Key requirements

Develop a program

275. Section 30AC provides that if an entity is the responsible entity for one or more critical infrastructure assets, the entity must adopt and maintain a critical infrastructure risk management program in relation to those assets. This requirement will ensure responsible entities develop a nuanced, comprehensive understanding of the threat picture that can affect the availability, confidentiality, reliability and integrity of the relevant critical infrastructure asset.

276. The risk management plan itself provides a tool for Government to verify whether the risk mitigation approach taken by the responsible entity is appropriate in protecting Australians' access to essential services.

277. It is not proposed that there be a one-size-fits-all approach to what amounts to an effective critical infrastructure risk management program. While the co-design process and Rules will provide further guidance on what issues must be addressed in a risk management plan, Government's intention is that responsible entities will have discretion as to how they construct their risk management program. This recognises industry's expertise and deep knowledge of the unique challenges faced by each critical infrastructure asset.

278. Failure to comply with this provision attracts a maximum civil penalty of 200 penalty units.

Comply with the program

279. Section 30AD provides that the responsible entity for one or more critical infrastructure assets must comply with the critical infrastructure risk management program it has adopted. This provision makes clear that while the process of developing a risk management program is important, the entity must then also take the necessary steps to implement that program.

280. Failure to comply with this provision attracts a maximum civil penalty of 200 penalty units.

Review and update the program

281. Sections 30AE and 30AF provides that the entity is also required to review the program on a regular basis and take all reasonable steps to ensure it is kept up to date. Meaningful uplift of the security and resilience of critical infrastructure will only occur if the risk management programs' articulation of material risks and mitigation strategies remain current. It is therefore vital that responsible entities review their risk management program on a regular basis and take reasonable steps to ensure it is kept up to date. This ensures risk is being continually assessed and managed by the entity rather than taking a set and forget approach to risk management.

282. The Bill does not define the frequency with which the review required in section 30AE must occur, but rather simply provides that it must occur on a regular basis. What is 'regular' for one asset may be different to another asset. This recognises that some assets face a significantly more fluid threat environment than others, and that changing circumstances should be the impetus for review rather than a strict mandated timeframe. Ultimately this will be a matter for the responsible entity to determine, however the Critical Infrastructure Centre will work with each sector to provide guidance on its expectations.

283. The Bill also does not define 'reasonable steps' in section 30AF, as it will depend on the individual circumstances of each entity. It is intended to ensure risk management programs are regularly reviewed and updated in response to evolving technology, business circumstances and changes in the threat environment.

284. Failure to comply with sections 30AE or 30AF attracts a maximum civil penalty of 200 penalty units.

Content of the program

285. Section 30AH sets out the requirements for a critical infrastructure risk management program. A critical risk management program is a written program that applies to a responsible entity for a critical infrastructure asset and the purpose of which is to do each of the following:

- Identify each hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset;
- So far as it is reasonably possible to do so – minimise or eliminate any material risk of such a hazard occurring; and
- Mitigate the relevant impact of such a hazard on the asset.

286. The program must comply with any requirements set out in the rules, which may be of general application or relate to a particular class of critical infrastructure asset.

287. A hazard in the context of a critical infrastructure risk management program is intended to mean an element which, alone or in combination with other elements, has the potential to give rise to risk. This broad interpretation is needed to reflect the diversity of critical infrastructure assets which will be subject to the obligation on commencement of the Bill, and into the future, and their evolving operating environment. Rather the focus should not be on the source of the hazard but its impact on the functioning of the asset.

288. A relevant impact is defined in section 8G to include the impact of the hazard on the availability, integrity, reliability or confidentiality of the asset, information about the asset, or data or information stored in the asset. Ultimately, this definition ensures responsible entities are considering how a particular hazard affects certain outcomes associated with the asset, whether or not there is a direct or immediate impact on business objectives.

289. What amounts to a material risk will ultimately be a matter for the responsible entity to determine by considering the likelihood of the hazard occurring and relevant impact of the hazard (subsection 30AH(6)). The approach to determining what is a 'material risk' is deliberately not prescriptive, in recognition of the many and varied risks faced by critical infrastructure assets and that businesses are best placed to themselves assess what might amount to a material risk. Further detail on this will be contained in sector-specific rules – see discussion below.

290. Noting these terms, the focus of the critical infrastructure risk management program is identifying and taking steps to minimise or eliminate any material risk arising from a hazard, or mitigating the impact of such a hazard. The requirements have been designed to align with existing business practices which would ordinarily consider the likelihood and consequence attaching to potential hazards business operations.

291. This approach is designed to achieve two key objectives:

a. Ensure the risk management program **does not** need to consider and take steps to address every potential hazard or risk. The focus is only on material risks.

b. Enable the business **to determine for itself** which risks are material and the appropriate measures to manage those risks.

Sector-specific rules

292. Part 2A imposes principled based obligations in recognition of the fact that a risk management program will vary radically between assets and sectors. As such, the process for developing a risk management program will be supported by co-designing sector-specific rules with industry and additional guidance provided by Government. The documents will provide requirements and guidance on meeting the obligations in the Bill.

293. Subsection 30AH(1)(c) specifically requires the critical infrastructure risk management program to comply with any requirements specified in the rules. At a minimum, it is proposed that sector-specific rules, to be developed with industry, will require responsible entities to consider and address risks in the following four domains:

a. *Physical security risks:* This includes risk of harm to people and damage to physical assets. For example, mechanical failures, natural hazards such as floods and cyclones, as well as human induced hazards such as terrorism.

b. *Cyber security risks:* Malicious cyber activity is one of the most significant threats facing Australian critical infrastructure assets and can range from denial of service attacks, to ransomware and targeted cyber intrusions.

c. *Personnel security risks:* This refers to the 'insider threat' or the risk of employees exploiting their legitimate access to an organisations' assets for unauthorised purposes including corporate espionage and sabotage.

d. *Supply chain risks:* The reliance on supply chains inherently involves dependencies on other assets, or providing other entities with some level of access to, or control of, your asset or business' deliverables. As is the case for personnel risk, supply chain risks relate to entities exploiting their legitimate access to, or control of, an organisations' assets for unauthorised purposes or otherwise creating a cascading impact to dependent assets.

294. In addition to deeming particular risks as material for the purposes of subsection 30AH(1)(b)(i), the rules may also:

- mandate the steps responsible entities should be taking through their risk management program to address these risks, including in relation to governance arrangements;
- recognise existing industry standards and practices are sufficient to meet aspects of the obligation; and
- de-conflict requirements for entities with assets which fall within more than one definition of critical infrastructure asset.

295. This approach will ensure Government is able to direct industry action in response to the changing threat environment.

296. Section 30AN makes clear that this may include applying, adopting or incorporating any matter contained in a law of a State or Territory or any matter contained in a standard proposed or approved by Standards Australia.

297. For example, in the electricity sector, the rules may draw upon the Australian Energy Sector Cyber Security Framework in outlining the steps necessary to manage cyber risks in the sector. Similarly, the rules could point to ISO standards as the basis for informing aspects of a risk management program.

298. All rules will be developed through extensive consultations, across industry and Government and will outline expectations, and what would be considered a reasonable and proportionate response

to meeting the obligations. This is supported by sections 30AL and 30AM which require appropriate consultation to occur prior to the making of any rules.

299. In the event there is an imminent threat that a hazard will have a significant relevant impact on a critical infrastructure asset, a rule may be made without consultation. However, in these circumstances, the Secretary must review the operation, effectiveness and implications of the rules within 60 days of the rules commencing. This review process must involve consultation with industry and the findings must be tabled in Parliament.

Background checking

300. Trusted insiders are potential, current or former employees or contractors who have legitimate access to information, techniques, technology, assets or premises. Trusted insiders can intentionally or unknowingly assist external parties in conducting activities against the organisation or can commit malicious acts of self-interest. Such action by a trusted insider can undermine or severely impact the availability, integrity, reliability or confidentiality of those assets captured as critical infrastructure assets.

301. Recognising the importance of personnel security, the Bill makes two key amendments to support industry's ability to understand and manage personnel security risks through background checking.

302. The Bill inserts new paragraph 8(1)(ba) into the *AusCheck Act 2007* to provide the ability for an AusCheck Scheme to be established in the regulations if the critical infrastructure risk management program requires background checking of individuals to be conducted under that scheme. Any such requirement for background checks of individuals under the critical infrastructure risk management program will be made by rules under new subsection 35AH(4).

303. These provisions mean that sector-specific rules can be made as part of the critical infrastructure risk management program to require backgrounds checks to be conducted under the AusCheck Scheme for certain individuals or employees that are involved in the operation of, or have access to, critical infrastructure assets. Accordingly, the requirements for background checking can be tailored to specific sectors and take into regard the unique challenges and threats faced by critical infrastructure assets.

304. Currently, AusCheck Schemes have been established to provide background checking services for the Aviation Security Identification Card (ASIC), Maritime Security Identification Card (MSIC), National Health Security (NHS) check schemes, and Major National Events (MNE), amongst others.

Annual reporting

305. Section 30AG provides that where a risk management plan is in place, the responsible entity of that critical infrastructure asset must provide a report to the Secretary of Home Affairs, or relevant Commonwealth regulator, within 30 days of the end of the financial year. The report must:

a. state whether or not the program was up to date during the financial year;

b. if a hazard had a significant relevant impact on one or more of those assets during the relevant period—includes a statement that identifies the hazard; evaluates the effectiveness of the program in mitigating the significant relevant impact of the hazard on the assets concerned; and outlines any variations made to the program as a result of the hazard occurring.

306. A relevant impact is defined in subsection 8G(1) as an impact on the availability, integrity, reliability or confidentiality of the asset. What is significant is likely to vary between assets and across sectors. It will be up to the entity to determine when a relevant impact is significant for the purposes of this reporting obligation, having regard to factors such as the extent of the impact, the

vulnerabilities it has exposed and any other factors the entity considers relevant. The Department will provide further guidance to support this particular obligation. It is not intended that entities will be required to report day-to-day incidents; instead the requirement will be to report incidents that have had, or risked having, a significant impact on the entity's ability to conduct its business or deliver its services.

307. This certification must be signed by each member of the board, council or other governing body, as the case requires. This is designed to ensure that the most senior levels of an entity are aware of the risk management practices of the entity and personally accountable compliance with this regime.

308. This obligation does not require the responsible entity to provide the full critical infrastructure risk management program to the Secretary, but rather is an assurance process to ensure that it remains up to date and appropriate.

309. Section 30AG also provides that failure to comply with the annual reporting obligation attracts a maximum penalty of 150 penalty units.

PART 2B - NOTIFICATION OF CYBER SECURITY INCIDENTS

310. During public consultation on the Cyber Security Strategy 2020 and these reforms, industry consistently advocated for increased information sharing on cyber threats. Industry has emphasised the need for Government and industry to be both providers and consumers of cyber intelligence to inform how networks can be best secured and how cyber resilience can be uplifted. The Australian Government must play a central coordination role in delivering an enhanced picture of cyber situational awareness, supported by the provision of cyber information by industry.

311. The third positive security obligation relates to the notification of cyber security incidents. The objective of this is to facilitate the development of an aggregated threat picture and comprehensive understanding of cyber security risks to critical infrastructure in a way that is mutually beneficial to Government and industry. Through greater awareness, the Government can better see malicious trends and campaigns which would not be apparent to an individual victim of an attack. This will support the Australian Government's investment in a national situational awareness capability and enhanced threat-sharing platform under the CESAR package.

312. This will better inform both proactive and reactive cyber response options – ranging from the Government issuing targeted guidance on preventing particular cyber attack methodologies, working with industry to uplift broader security standards and providing immediate assistance to industry in response to an incident.

313. Similarly to the other positive security obligations, section 30BB provides a mechanism by which the Minister for Home Affairs, through making rules, can activate the obligation for particular critical infrastructure assets. This 'on-switch' is intended to prevent duplication should an existing, equivalent, obligation exist under another regulatory regime.

314. Where activated, the obligation imposes a two-tiered reporting obligation on the responsible entity for a critical infrastructure asset based on the severity of the cyber security incident. The reports must be made to the Australian Signals Directorate (unless another Commonwealth body is prescribed in the rules), and made orally or in writing. The Secretary of Home Affairs will provide an approved form for the written report or record of the oral report.

315. Failure of the responsible entity to provide a report consistent with either of these obligations may result in a civil penalty of up to 50 penalty units.

316. Where a report is made, an entity or an officer, employee or agent of an entity, is not liable to any civil action for doing so. These immunities are intended to encourage responsible entities to cooperate fulsomely with Government and provide timely and meaningful information to the relevant Commonwealth body.

Critical cyber security incidents

317. Section 30BC provides that a responsible entity must report a critical cyber security incident within 12 hours of the entity become aware that the incident met the critical criteria. To be critical, a cyber security incident must have occurred or be occurring and have had, or be having, a significant impact on the availability of the asset.

318. A cyber security incident is defined in section 12M as one or more acts, events or circumstances involving unauthorised access, modification or impairment of computer data, a computer program or a computer.

319. Determining whether an incident is having a significant impact on the availability of the asset will be matter of judgment for the responsible entity however the Critical Infrastructure Centre will issue sector specific guidance to assist in this determination. This threshold has been left intentionally undefined as the significance of an impact on the availability of an asset will vary radically between assets. For example, a cyber security incident which affects the availability of a critical clearing and settlement facility for a very brief period may have significant economic repercussions while an incident that affects the availability of a critical education asset for the same period of time may have a substantially lower impact. The services being provided by the asset, together with the nature and extent of the cyber security incident, will determine the significance of incident and whether it meets the threshold of being a critical cyber security incident. It is not intended that day-to-day incidents, such as the receipt of a scam email, should be reported as they would not meet the level of significance required.

320. An investigation of an outage may take time to occur before it can be determined that its source was a cyber security incident, as opposed to for example a mechanical failure. In light of this, the obligation to report within 12 hours is only enlivened when the responsible entity becomes aware that the incident meets the above criteria. In doing so, the obligations requires the notification of Government to be one of the first steps in the businesses incident response plan.

Other cyber security incidents

321. Section 30BD provides the second tier of the reporting obligation. Under this section, the responsible entity must report, within 24 hours, where:

- a cyber security incident has occurred, is occurring, or is imminent; and
- the incident has had, is having, or is likely to have, a relevant impact on the asset.

322. A relevant impact in this context is defined in subsection 8G(2) to mean an impact on the availability, integrity, reliability or confidentiality of the asset. By contrast to a critical cyber security incident, this obligation relates to any impact on availability (irrespective of the significance) alongside the other forms of impact. This may include incidents such as compromises of a computer system where the malicious actor is yet to interfere with the operation of the asset, data theft and exfiltration, or persistent targeting or attempted access to a network where the entity believes a compromise is imminent.

323. Similarly to critical cyber security incidents, the responsible entity is only required to report when the entity becomes aware that the incident meets the above criteria. This means that the obligation may not be enlivened until after an investigation of the impact has occurred, or the

compromise has been discovered. While these events may have minimal immediate impact on the customers or delivery of the essential services of the asset, they demonstrate a concerning compromise, or imminent compromise, of the critical infrastructure assets computer network.

PART 2C – ENHANCED CYBER SECURITY OBLIGATIONS

324. Critical infrastructure assets and the systems they rely on are increasingly interconnected and interdependent. While Parts 2, 2A, and 2B, discussed above, impose obligations to manage risks to the operation of these assets, a small subset of critical infrastructure assets are of the highest criticality due to their interdependences with other critical assets. A closer partnership is required in relation to these systems of national significance, and the computer infrastructure that underpins them, to build enhanced cyber resilience and preparedness.

325. The Australian Government has introduced the enhanced cyber security obligations to strengthen the cyber preparedness and resilience of entities that operate critical infrastructure assets of the highest criticality (system of national significance). Consultation on the Cyber Security Strategy 2020 supported initiatives to enhance cyber information sharing to build a stronger collective understanding of threats to Australian systems. These obligations enable the Government to establish a bespoke partnership, tailored to individual assets, to not only prepare entities to better manage cyber risks but also improve Australia's situational awareness, particularly as the threat environment worsens.

326. Under Part 6A, the Minister for Home Affairs may declare a critical infrastructure asset to be a system of national significance. Part 2C provides for a series of enhanced cyber security obligations which may be imposed on the responsible entity for a system of national significance. Responsible entities for systems of national significance will not be obligated to comply with each of these enhanced obligations following the Minister's declaration, but rather may be required to do so, from time to time, following a written notice from the Secretary of Home Affairs. This approach reflects the different nature of the obligations provided under this Part, which are aimed at addressing or identifying vulnerabilities and building resilient practices.

327. The Australian Government will continue to build on the strong voluntary engagement and cooperation with critical infrastructure entities that has underpinned the success of the relationship to date. This includes providing voluntary support and guidance. However, there may be instances where entities are unwilling or unable to voluntarily cooperate and the Enhanced Cyber Security Obligations are necessary.

<u>Division 2 of Part 2C – Statutory incident response planning obligations</u>

328. The first of the enhanced cyber security obligations which the Secretary may require the responsible entity for a system of national significance to comply with is the statutory incident response planning obligation. Incident response plans are designed to ensure an entity has established processes and tools to prepare for and respond to cyber security incidents. Incident response plans will provide assurance to Government that entities are sufficiently prepared for cyber security incidents and will assist entities by clearly articulating 'what to do' and 'who to call' in the event of a cyber security incident. Clear escalation pathways and processes can be crucial to mitigating and minimising the consequences of fast moving cyber incidents.

329. Section 30CB enables the Secretary of Home Affairs to determine that the statutory incident response planning obligations apply to the entity, meaning that it must adopt and maintain an incident response plan (section 30CD), comply with the plan (section 30CE), and regularly review (section 30CF) and take all reasonable steps to ensure the plan is up to date (section 30CG).

330. Section 30CJ provides that an incident response plan is a written plan that relates to the system of national significance, for the purposes of planning for responding to cyber security incidents

that could have a relevant impact on the system. The plan must comply with any requirements specified in the rules, which may include details on procedures to be included in the plan for responding to a particular cyber security incident.

331. Incident response plans will vary from entity to entity. However common elements of an incident response plan include definitions of the types of systems being used, details of staff member roles and responsibilities, outlines of common cyber incidents and incident response processes to mitigate and remediate a cyber security incident.

332. A copy of the incident response plan must be provided to the Secretary of Home Affairs, as soon as practicable after it is adopted or varied. This will ensure Government and entities have the necessary information to activate cyber security incident response arrangements at any point in time, particularly in the event of an emergency.

333. A civil penalty of up to 200 penalty units applies for failure to comply with the obligations in this Division.

Division 3 of Part 2C – Cyber security exercises

334. The second of the enhanced cyber security obligations which the Secretary may require the responsible entity for a system of national significance to comply with is the requirement to undertake a cyber security exercise.

335. Cyber security exercises are an integral part of an entity's cyber security procedures, as they are used to test response preparedness, mitigation and response capabilities. Such exercises enable an entity to develop an understanding of how to address a cyber incident through a scenario that requires the entity to draw upon resources, such as incident response plans, relevant legislation, policies and processes to identify the most appropriate response to a cyber security incident. Cyber security exercises can identify gaps in existing approaches and help streamline processes to ensure more effective and efficient responses to threats as they emerge.

336. During consultation on the Cyber Security Strategy 2020, submissions highlighted the importance of joint cyber security exercises involving industry and government to improve entities' cyber resilience. Noting the interdependencies between critical infrastructure assets, these exercises can be used to develop interoperable response capabilities to prevent a cascading of impacts across sectors.

337. Section 30CM provides that the Secretary of Home Affairs may, by written notice, require the entity to undertake a cyber security exercise in relation to all types of cyber security incidents, or one or more specified types of cyber security incidents (for example, a denial of service or ransomware attack). The scope of the exercise will be determined based on analysis of threats and incident trends, as well as consideration of the consequential or cascading effects that may occur should the system be impacted by a cyber security incident.

338. A cyber security exercise is defined in section 30CS to an exercise, the purpose of which is to test the entity's:

- ability to respond appropriately to the cyber security incident/s;
- preparedness to response appropriately to the cyber security incident/s; and
- ability to mitigate the relevant impacts the cyber security incident/s could have on the system.

339. Cyber security exercises are generally conducted through one of two formats: discussion-based or tabletop exercises, and operational or functional exercises.

340. The Secretary of Home Affairs may also require that the entity allow specified designated officers to observe the cyber security exercise, provide those officers with access to the premises or other assistance and facilities to allow the observation of the exercise, allow them to make reasonably necessary records and give them notice of when the exercise will commence. A designated officer is defined in section 30DQ to be an employee of the Department of Home Affairs or a staff member of the Australian Signals Directorate.

341. Section 30CQ provides that, on completion of the exercise, the entity is required to prepare an evaluation report relating to the exercise and give a copy of the report to the Secretary. An evaluation report is a written report the purpose of which is to evaluate the entity's:

- ability to respond appropriately to the cyber security incident/s;
- preparedness to respond appropriately to the cyber security incident/s, and
- ability to mitigate the relevant impacts the cyber security incident/s could have on the system.

342. However, if the entity has prepared, or purported to prepare an evaluation report, provided it to the Secretary for Home Affairs and the Secretary has reasonable grounds to believe that the report was not prepared appropriately, the Secretary may require the entity to appoint an external auditor to prepare an evaluation report for the entity. Alternatively, if the entity fails to comply with section 30CQ the Secretary for Home Affairs may require an external evaluation report to be prepared by an external auditor. An external auditor is a specified individual authorised by the Secretary as such for the purposes of the Act.

343. A civil penalty of up to 200 penalty units applies for failure to comply with the obligations in this Division.

Division 4 of Part 2C – Vulnerability assessments

344. The third element of the enhanced cyber security obligations which the Secretary may require the responsible entity for a system of national significance to comply with is the requirement to undertake a vulnerability assessment.

345. Vulnerability assessments are a routine cyber security practice undertaken to identify vulnerabilities or 'gaps' in systems which expose them to particular types of cyber incidents. These preparatory activities also enable the entity to evaluate the risk of particular vulnerabilities. This will enable entities that operate Australia's systems of national significance to remediate vulnerabilities before they can be exploited by malicious actors. The identification of vulnerabilities in one system may also enable the remediation of similar vulnerabilities across other critical systems.

346. A vulnerability assessment can consist of a documentation-based review of a system's design, a hands-on assessment or automated scanning with software tools. In each case, the goal is to identify security vulnerabilities.

347. Section 30CU provides that the Secretary of Home Affairs may require the entity to undertake, or cause to be undertaken, a vulnerability assessment in relation to the system and a particular type of cyber security incident, or cyber security incidents generally. The entity need not undertake the assessment themselves, but may rather chose to engage the services of a third party to undertake the assessment. Prior to making such a request, the Secretary is required to consult with the entity. This consultation requirement will assist the Secretary to determine the entities capacity to undertake, or cause to be undertaken, the required vulnerability assessment.

348. If the Secretary of Home Affairs has reasonable grounds to believe that the entity would not be capable of complying with a notice or has not complied with an earlier notice, the Secretary may

give a designated officer a written request to undertake the vulnerability assessment and require the entity to provide reasonable access, assistance and facilities to the officer to allow the assessment to be undertaken.

349. If the entity, or a designated officer, undertakes a vulnerability assessment they must prepare, or cause to be prepared, a vulnerability assessment report and provide a copy of the report to the Secretary.

350. A civil penalty of up to 200 penalty units applies for failure to comply with the obligations in this Division.

Division 5 of Part 2C – Access to system information

351. The final of the enhanced cyber security obligations which the Secretary may require the responsible entity for a system of national significance to comply with is the requirement to provide system information.

352. During consultation on the Cyber Security Strategy 2020, stakeholders strongly supported initiatives to improve information sharing to make critical infrastructure more resilient and secure. The provision of system telemetry from systems of national significance will support the Government's ability to build a near-real time threat picture through the CESAR capability and share actionable, anonymised information back out to industry. Aggregated system information, overlaid with intelligence and reporting, will also enable the Government to target its limited capabilities to the threats and vulnerabilities of greatest consequence to the nation.

353. System information is information that relates to the operation of the computer needed to operate a system of national significance which may assist with determining whether a power under this Act should be exercised in relation to the system of national significance, in particular the powers set out in Part 3A. System information however does not include personal information within the meaning of the *Privacy Act 1988*. For example, system information may be network logs or alerts that provide visibility of the operation and functioning of a broader computer network. The monitoring of this information can be crucial to identifying a compromise of a system and deploying a rapid response to mitigating its potential impacts.

354. Section 30DB provides that, if the Secretary of Home Affairs believes on reasonable grounds that the responsible entity for the system of national significance is technically capable of doing so, the Secretary may require the entity to provide the Australian Signals Directorate with periodic reports consisting of specified system information ('a system information periodic reporting notice'). The Secretary may specify the intervals, manner and form in which the information is to be provided, as well as any other information technology requirements relating to the provision of the information. Depending on the information required and the ability for automated provision (such as automated machine-to-machine cyber threat intelligence sharing), these reports may be required to be made at rapid intervals, for example, every minute.

355. Section 30DC provides that, if the Secretary of Home Affairs believes, on reasonable grounds, that the responsible entity for the system of national significance is technically capable of doing so, the Secretary may require the entity to provide the Australian Signals Directorate with reports consisting of specified system information as soon as practicable after each incidence of a specified event occurring ('a system information periodic reporting notice'). For example, a report may be required every time a particular computer program raises a specified class of alert or error message.

356. In deciding whether to give a system information periodic reporting notice or a system information event-based reporting notice, the Secretary of Home Affairs must have regard to the costs that are likely to be incurred by the entity in complying with the notice. To support this consideration as well as the determination of whether the entity is technically capable of

providing the report, section 30DD mandates that the Secretary of Home Affairs must consult with the entity prior to issuing the notice.

357. If the Secretary of Home Affairs does not believe on reasonable grounds that the entity would be technically capable of preparing reports under sections 30DB or 30DC, section 30DJ provides that the Secretary may require the entity to install and maintain a specified computer program ('system information software notice'). The computer program may only be specified in the notice if its purpose is to collect and record the required system information and cause the information to be transmitted electronically to the Australian Signals Directorate. The computer program will be provided by the Government and will, for example, operate as a host-based sensor reporting back to the Australian Signals Directorate telemetry information used to monitor the system for malicious behaviour.

358. In deciding whether to give a system information software notice, the Secretary of Home Affairs must have regard to the costs that are likely to be incurred by the entity in complying with the notice. To support this consideration, section 30DK mandates that the Secretary of Home Affairs must consult with the entity prior to issuing the notice.

359. A civil penalty of up to 200 penalty units applies for failure to comply with the obligations in this Division.

PART 3A – RESPONDING TO SERIOUS CYBER SECURITY INCIDENTS

360. Parts 2A, 2B, 2C, discussed above, impose obligations on industry to manage risks associated with the operation of critical infrastructure assets. However, where serious risks do eventuate which affect the ability of the asset to deliver essential services and prejudice Australia's national interests, effective mechanisms are required to resolve the incident.

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

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

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

Ukraine power outages, 2015

The 23 December 2015 Ukrainian power outages highlighted the potential impacts of cyber attacks on critical infrastructure. The attack involved sophisticated malicious actors taking command and control of the Supervisory Control and Data Acquisition networks of three energy distributors,

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

WannaCry, 2017

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

Hospital attacks, 2020

Since the COVID-19 pandemic began, hospitals have come under increasing strain due to malicious cyber incidents, particularly ransomware attacks. The March 2020 ransomware attack on Brno University Hospital, one of Czechia's largest COVID-19 testing laboratories, saw the forced shut down of its entire information technology network. In September 2020, Dusseldorf University Hospital suffered a ransomware attack that brought down its computer systems. As a result, an individual being transported to the hospital by ambulance was re-routed to another hospital 30 kilometres and passed away en route.

363. Part 3A provides an emergency mechanism by which the Government can appropriately respond to the most serious of cyber security incidents which are affecting critical infrastructure assets and where the relevant entity is unwilling or unable to do so. The mechanism is subject to a range of stringent safeguards and limitations to ensure it is only used in the most serious circumstances and in an appropriate way.

When can these powers be used?

364. Part 35AB establishes the circumstances of which the Minister for Home Affairs must be satisfied before being able to authorise any actions under the regime. Firstly, subsection 35AB(1)(a) provides that a cyber security incident must have occurred, be occurring or be imminent. A cyber security incident is defined in section 12M as one or more acts, events or circumstances involving unauthorised access, modification or impairment of computer data, a computer program or a computer.

365. Secondly, subsection 35AB(1)(b) requires that the incident has had, is having or is likely to have a relevant impact on a critical infrastructure asset. Subsection 8G(2) provides the definition of a relevant impact in this context, which includes an impact on the availability, integrity, reliability or confidentiality of the asset. This limb is important to ensure that the regime can only be used to protect Australia's critical infrastructure assets.

366. Thirdly, subsection 35AB(1)(c) provides that there must be a material risk that the incident has seriously prejudiced, is seriously prejudicing, or is likely to seriously prejudice:

- the social or economic stability of Australia or its people; or

- the defence of Australia; or
- national security.

367. This requirement ensures that the regime can only be used in the most serious of circumstances where Australia's national interests are being seriously prejudiced. In such circumstances, the Government's responsibility to protect Australia's national interests are engaged.

368. Finally, subsection 35AB(1)(d) provides that the Minister for Home Affairs must also be satisfied that no existing regulatory system of the Commonwealth, a State or a Territory could be used to provide a practical and effective response to the incident. This limb further embeds the last resort nature of this regime by ensuring it is only used when other regimes, which are potentially less invasive or which are designed specifically to address risks associate with particular assets, are not appropriate.

Hypothetical scenario:

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

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

What can be authorised?

369. In such circumstances, the Minister for Home Affairs may authorise the Secretary of Home Affairs do one or more of the following:

- give directions to a specified entity for the purposes of gathering information;
- give specified directions to a specified entity requiring the entity do one or more acts or things in response to the incident; or
- give a request to the authorised agency to provide specified assistance and cooperation to response to the incident.

370. The Minister for Home Affairs may authorise any combination of the above concurrently or successively following further applications. To support the Minister in determining whether the circumstances in subsection 35AB(1) exist, an authorisation for an action direction or intervention request is reasonably necessary and proportionate, and that the entity is otherwise unwilling or unable to take all reasonably necessary steps to appropriately respond to the incident, the Minister must consult the effected entity unless the delay would frustrate the effectiveness of the Ministerial authorisation (section 35AD).

371. The Minister for Home Affairs must provide a copy of the authorisation, or a record of an oral authorisation, to the following persons:

- The Secretary of Home Affairs - this will ensure that the Secretary has a clear understanding of what exactly has been authorised.

- The Inspector-General of Intelligence and Security - to provide them with visibility of the decision noting their important oversight role in relation to intervention requests.

- The specified relevant entity for the asset – to provide them with a clear understanding of what has been authorised and allow them to ensure that any actions taken under the authorisation are consistent.

372. Section 35AG provides that, when making the authorisation, the Minister for Home Affairs must specify the period for which the notification is to remain in force. This period must not exceed 20 days.

373. If the authorisation is required beyond the originally specified period, the Minister for Home Affairs must make a fresh authorisation, and being satisfied of the various factors set out in section 35AB, must also have regard to the number of occasions on which Ministerial authorisations have been made in relation to the incident and the asset.

374. To ensure the Ministerial authorisation is not in place for any longer than is necessary, section 35AH imposes an obligation on the Minister for Home Affairs to revoke the authorisation if the Minister is no longer satisfied that it is no longer required to respond to the incident. To support this obligation, the Secretary of Home Affairs also has an obligation to notify the Minister if the authorisation is no longer required.

Information gathering directions

375. The cyber infrastructure relied on by many critical infrastructure assets, which may be the potential target of a cyber attack, is often complex. Equally, the methods of exploitation that may be adopted by a malicious actor may be highly sophisticated and obscure the methodology of the attack. Therefore information is crucial to determining how to effectively respond to a cyber security incident.

376. The Secretary of Home Affairs has information gathering powers in section 37 of the SOCI Act which may be relied on to gather information from a critical infrastructure asset to support the Minister for Home Affairs' decision as to whether the criteria set out in subsection 35AB(1) are met. However, when satisfied of these criteria, further information may still be required to determine the most appropriate response and the relevant entities willingness or ability to take all reasonably necessary steps to affect such a response.

377. Noting the complex and far-reaching aspects of a computer network which supports a critical infrastructure asset, the responsible entity for the asset may not always have the necessary information or ability to acquire it. Rather the direction must be able to be made in relation to the entity that is best placed to respond. Therefore, this authorisation may be made in relation to a relevant entity for the critical infrastructure asset or another related asset within a critical infrastructure sector. A relevant entity is defined in section 5 as an entity that is the responsible entity for the asset, is a direct interest holder in relation to the asset, is an operator of the asset, or is a managed service provider for the asset.

378. Further, although the regime is focused on supporting a critical infrastructure asset in the prevention of a cyber security incident, mitigating the impacts of such an incident, or restoring the functioning of the asset following an incident, it may be necessary to gather information in relation to other critical infrastructure sector assets to assist with this response. For example, a critical infrastructure sector asset may be the target of the attack and due to a crucial interdependency, the operation of that critical infrastructure sector asset is having a relevant impact on the primary critical infrastructure asset. Alternatively, a critical infrastructure sector asset may be the vector of the attack on the primary critical infrastructure asset or be in a position to assist with responding to the incident. This approach ensures that authorisations may be made

in relation to assets at the necessary point in the critical infrastructure assets supply chain or in relation to interdependent assets within the broader critical sector.

379. In light of the above factors, subsection 35AB(2)(a) and (b) provide that the Minister for Home Affairs may authorise the Secretary of Home Affairs to give directions under section 35AK (information gathering directions) to a relevant entity which is specified in the authorisation in relation to a particular asset, whether it is the critical infrastructure asset (the primary asset) or another asset in a critical infrastructure sector which relates to the primary asset.

380. However, the Minister for Home Affairs must not authorise information gather directions unless satisfied that doing so is likely to facilitate a practical and effective response to the incident.

381. If the Minister for Home Affairs makes such an authorisation, and the Secretary of Home Affairs has reason to believe that the entity has information that may assist with determining whether a power under the Act should be exercised in relation to the incident and the asset, the Secretary of Home Affairs may direct the entity to give any such information.

382. Consistent with the power in section 37 of the SOCI Act, if the entity fails to comply with a direction under section 35AK to the extent the entity is capable of doing so, the entity may be liable to a civil penalty of 150 penalty units.

383. Reflecting the nature of this direction making power, and noting the consequences of failing to comply with a direction, there are a range of additional safeguards which apply.

384. The Secretary of Home Affairs must not give a direction unless satisfied that the direction is a proportionate means of obtaining the information and compliance with the direction is technically feasible (subsection 35AK(4)). A direction is technically feasible when the direction relates to a course of action that is reasonably possible to execute, or within the existing capability of the relevant entity. A direction is considered not to be technically feasible if there is no technical capability that could be utilised to produce the outcome that is sought.

385. Further, subsection 35AK(5) prevents the Secretary of Home Affairs from issuing a direction that would require an entity to do certain acts or thing that are prohibited under the *Telecommunications (Interception and Access) Act 1979* – specifically intercept communications or provide access to stored communications. Subsection 35AK(5) also ensures that a direction cannot be issued if it requires an entity to disclose communications or telecommunications data that is protected under sections 276, 277 and 278 of the *Telecommunications Act 1997*.

386. To support the Secretary of Home Affairs in determining whether the entity has information that may assist in determining whether a power under the Act should be exercised and whether compliance with the direction would be proportionate and technically feasible, subsection 35AK(6) requires the Secretary of Home Affairs to consult the entity prior to making the direction unless the delay would frustrate the effectiveness of the direction. This consultation will allow the entity to indicate whether compliance with a proposed direction would not be possible or otherwise indicate difficulties with complying.

387. Further, while the entity is not excused from giving information in response to a direction because the information would potentially incriminate the entity, any information provided is not admissible in evidence against the entity except in relation to proceedings for providing false or misleading information or documents and failing to comply with the direction. This reflects that the purpose of information gathering power is not to investigate an offence, or pursue any investigation against the entity, but rather, to better understand the situation to facilitate a better response to the incident.

Hypothetical scenario:

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

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

Action directions

388. Once the Minister for Home Affairs is aware of the acts or things required to effectively respond to the incident, the Minister may, under paragraphs 35AB(2)(c) and (d), authorise the Secretary of Home Affairs to give a specified entity a specified direction. This power is similar to that in section 32 of the SOCI Act, however, can be applied more readily within emergency situations.

389. Reflective of the significance of this power, and the criminal penalty that attaches to non-compliance, it is subject to strong safeguards and limitations.

390. Firstly, paragraph 35AB(7)(a) provides that the Minister for Home Affairs must be satisfied that the entity is unwilling or unable to take all reasonably necessary steps to appropriately resolve the incident. The owner or operator of the asset has primary responsibility for the asset, with the Government's responsibility only being enlivened whether their willingness or inability to response to an incident is having flow on impacts to Australia's national interests. This safeguard is central to establishing this regime as one of last resort, as the Government will only intervene when the entity itself has failed to do so. The use of the term 'reasonably necessary steps' is intended to provide clarity that the entity is not required to take steps which are disproportionate or reckless in responding to the incident. Rather an entity may be prevented from taking the necessary actions due to contractual obligations (for example, an obligation on a data centre to not prevent a customer accessing their data stored data) or may not have the technical expertise to respond to an attack from a highly sophisticated actor (for example, their records have been encrypted and the entity does not have back-ups).

391. Secondly, paragraph 35AB(7)(b) provides that the Minister for Home Affairs must not give an authorisation in relation to an action direction unless the Minister is satisfied that the specified direction is reasonably necessary for the purposes of responding to the incident. It is not possible to accurately foresee the many ways a system may be compromised or the actions that would be required to respond to the incident. Therefore, the Minister for Home Affairs' power to authorise the giving of a direction for the entity to do, or refrain from doing, a specified act or thing is left intentionally broad. However the safeguards at paragraphs 35AB(7)(b) and (c) (discussed below) operate to ensure that it only permits directions being made that amount to an appropriate response to the cyber security incident. Section 12P provides examples of responding to a cyber security incident, which include preventing the incident, mitigating its impacts, and restoring the functionality of the asset.

392. The scope of conduct that can be authorised is further limited by subsection 35AB(9) which expressly prohibits the Minister for Home Affairs authorising certain actions. The Minister must not use this power as an alternative pathway for actions that are covered by section 35AX. Further the Minister must not require the entity to take offensive cyber action against a person who is directly or indirectly responsible for the incident. This regime is exclusively focused on protecting

and defending the asset and cannot be used to compel an entity to undertake disruptions outside their own networks. Should such actions be necessary and appropriate in the circumstances, the *Intelligence Services Act 2001* provides a complementary regime whereby the Australian Signals Directorate may undertake such activities offshore under stringent oversight arrangements.

393. Thirdly, paragraph 35AB(7)(c) provides that the Minister for Home Affairs must be satisfied that the specified direction is a proportionate response to the incident. This will ensure that the acts or things required to be done are balanced against factors such as the consequences of doing so, the responsibilities of the entity, the services the asset provides. For example, while taking a computer network offline would prevent an imminent attack, it may not be regarded as proportionate if doing so would lead to widespread power loss to a city.

394. Finally, paragraph 35AB(7)(d) provides that the Minister for Home Affairs must be satisfied that compliance with the specified direction is technically feasible to ensure that the entity is not compelled to do something they are technically unable to do. A direction is technically feasible when the direction relates to a course of action that is reasonably possible to execute, or within the existing capability of the relevant entity. A direction is considered not to be technically feasible if there is no technical capability that could be utilised to produce the outcome that is sought. To support the Minister for Home Affairs' understanding of the technical capabilities of the relevant entity, the Minister is required to consult the effected entity unless the delay would frustrate the effectiveness of the Ministerial authorisation (section 35AD).

395. Prior to giving a Ministerial authorisation for an intervention request, the Minister for Home Affairs is required to consult the responsible entity for the critical infrastructure asset or the owner or operator, whoever is considered to be most relevant, of the critical infrastructure sector asset. When a Ministerial authorisation is made, under section 35AQ the Secretary of Home Affairs may give the entity a specific direction (authorised by the Minister) including the timeframe in which the entity is required to do the act or thing.

396. Compliance with such a direction takes precedence over other obligations in the Act. For example, if the asset in question is also a system of national significance and the entity is under an obligation to provide system information as a result of a notice issued under subsection 30DB(2), if compliance with the direction would prevent them from providing the information at the required intervals, the entity would not be liable to a breach of that obligation.

397. Further, the entity, or its officer, employee or agent, is not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith in compliance with a direction given under section 35AQ. This immunity will protect the entity from any civil claims that may arise as a result of complying with the direction. For example, where the entity was contractually obliged to provide the customer continuous access to a service and the direction required that access to be interrupted, the entity is not liable for any civil action initiated by the customer in relation to breaching that obligation.

Hypothetical scenario*:*

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

The Minister for Home Affairs may authorise the Secretary to direct the entity to segregate the compromised computer.

Intervention requests

398. The final type of Ministerial authorisation relates to situations where directing the entity to do the act or thing would not be practical or effective (for example, the entity is unwilling or unable to comply), and the Government is require to step in to do the act or thing. In such circumstance, the Minister for Home Affairs may authorise the Secretary of Home Affairs to give a specified request to the authorised agency in relation to the incident and specified asset. The authorised agency is defined as the Australian Signals Directorate (which includes the ACSC), which is Government's premier cyber expert and has the capability to respond to critical cyber security incidents.

399. Reflective of the significance of this power it is subject to even more robust safeguards and limitations than those applicable to action directions.

400. Firstly, paragraph 35AB(10)(a) provides that the Minister for Home Affairs must not make the authorisation if an authorisation for an action direction would not amount to a practical and effective response to the incident. This criterion ensures that this invasive power is strictly reserved for last resort situations where directing the entity to do the required act or thing would not work. For example, a direction may have been issued and the entity refused to comply or, as a result of consultation with the entity as required under section 35AD, the Minister is aware that the entity is not technically capable of undertaking the necessary action.

401. Secondly, paragraphs 35AB(10)(b) and (c) provides that the Minister for Home Affairs must be satisfied that the entity is unwilling or unable to take all reasonably necessary steps to appropriately resolve the incident. This safeguard builds on paragraph 35AB(10)(b) and further supports this regime as one of last resort in that the entity has principle responsibility for responding to the incident. The Government's responsibility is only enlivened when the entity's willingness or inability to respond to the incident is having flow on impacts to Australia's national interests. The use of the term 'reasonably necessary steps' is intended to provide clarity that the entity is not required to take steps which are disproportionate or reckless in responding to the incident. Rather an entity may be prevented from taking the necessary actions due to contractual obligations (for example, an obligation on a data centre to not prevent a customer accessing their data stored data) or may not have the technical expertise to respond to an attack from a highly sophisticated actor (for example, their records have been encrypted and the entity does not have back-ups).

402. Thirdly, paragraph 35AB(10)(d) provides that the Minister for Home Affairs must not make such an authorisation unless the Minister for Home Affairs is satisfied that the specified request is reasonably necessary for the purposes of responding to the incident. Similarly to paragraph 35AB(7)(a), this safeguard ensures that requested actions are strictly targeted at responding to the incident. Subsection 35AB(12) expressly excludes the Minister for Home Affairs authorising a request which would involve the authorised agency taking offensive cyber action. This regime is exclusively focused on the defence and protection of the asset.

403. Fourthly, paragraph 35AB(10)(e) provides that the Minister for Home Affairs must be satisfied that the specified request is a proportionate response to the incident. This will ensure that the acts or things required to be done are balanced against factors such as the consequences of doing so, the responsibilities of the entity, the services the asset provides. In this instance, the Minister will consider the consequence of the Government directly intervening to take the action, as well as the potentially consequences of that action.

404. Fifthly, the act or thing must be of a kind covered by section 35AC. This condition serves as another limiter to ensure that the actions are computer-related acts and appropriately targeted as responding to the cyber security incident and reflect the specialised skills of the authorised agency which in many circumstances surpass those of the private sector. The requests authorised by the Minister for Home Affairs, and made by the Secretary could include:

- Access to a computer – for example, the request may specify that the authorised agency access, either locally or remotely, the supervisory control and data acquisition (SCADA) system of an asset to support incident response.

- Undertake an analysis of computer data – for example, the request may specify that the authorised agency analysis the networks logs of a specified period to determine the exact time and nature of the unauthorised access to the computer, and deploy investigative tools to a network to enable the analysis of computer data.

- Alter data held in a computer – for example, the request may specify that the authorised agency is to reconfigure the password of a particular operating system to prevent further compromises. The request may also specify that the authorised agency is able to remove, alter, and/or delete malicious software operating on the network to enable defensive actions.

- Alter the functioning of a computer – for example, the request may specify that the authorised agency is to segregate a particular server to prevent a malicious actor who has compromised the network from gaining access to particular computer data and programs in order to mitigate the impacts of the incident or enable blocking of malicious cyber activity on computers and at the network perimeter and/or with the provider of IT services to that network.

Hypothetical Scenario:

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

To remediate the cyber security incident, the authorised agency may need to remove malicious software (e.g. web shells, ransomware, and/or reconnaissance tools) which requires altering/removing of data in a computer. The authorised agency may need to conduct these activities on-site with the victim or remotely, where capability exists to do so.

The authorised agency may also implement blocking of malicious domains, may disable internet access or may implement other specified mitigations. The authorised agency may also require systems to be patched (altering data) or a change in network configurations, to alter the function of the system, to prevent a similar activity.

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

405. Finally, paragraph 35AB(10)(f) provides that the Minister for Home Affairs must be satisfied that compliance with the specified request is technically feasible. A request is technically feasible when the request relates to a course of action that is reasonably possible to execute, or within the existing capability of the authorised agency. A direction is considered not to be technically feasible if there is no technical capability that could be utilised to produce the outcome that is sought. This will prevent futile or unreasonable requests being made of the authorised agency.

406. The Minister for Home Affairs must also obtain the agreement of the Prime Minister and Defence Minister prior to authorising an intervention request. The Prime Minister, as leader of the country and chair of the National Security Committee of Cabinet, is well positioned to assess the appropriateness of such an authorisation. The Defence Minister, as the minister responsible for the authorised agency, will ensure that their involvement is appropriate.

407. When a Ministerial authorisation is made, under section 35AX the Secretary of Home Affairs may give the chief executive of the authorised agency a request that the agency do one or more acts or things that are specified in the authorisation. Section 35AZ then provides the authorised agency authority to do an act or thing in compliance with the request made by the Secretary of Home Affairs and clarifies that acts or things done in compliance are consistent with the authorised agency's functions in section 7(1)(f) of the *Intelligence Services Act 2001*. It is intended that the Department of Home Affairs will be prescribed through regulations as a Commonwealth authority for the purposes of paragraph 13A(1)(c) of the *Intelligence Services Act 2001*.

408. Importantly, subsection 35AX(5) prevents the Secretary of Home Affairs from requesting an authorised agency to do an act or thing that is prohibited under the *Telecommunications (Interception and Access) Act 1979* – specifically intercept communications or access to stored communications. Subsection 35AX(5) also ensures that a request cannot be issued if it allows an authorised agency to access communications or telecommunications data that is protected under sections 276, 277 and 278 of the *Telecommunications Act 1997*.

409. The Inspector-General of Intelligence and Security has extensive powers to oversee the actions of the authorised agency and will be able to do so in relation to these actions. To assist with this oversight role, the Inspector-General will be notified when a Ministerial authorisation is made.

410. The relevant entity for the asset is required under section 35BB to provide the staff member of the authorised agency with access to premises for the purpose of complying with the request and provide specified information or assistance that is reasonably necessary to allow the authorised agency to comply with the request. Reasonable assistance may include things such as identifying a particular server of interest to the staff member or explaining how to access a particular computer program. A civil penalty of up to 150 penalty units applies for failure to provide such assistance.

411. If the entity refuses or fails to provide access to the premises, or part of the premises, section 35BC provides that a constable may use reasonable force against property for the purposes of assisting the staff member of the authorised agency to comply with the Secretary of Home Affairs' request.

412. Constables are trained in the use of force against property and are subject to various oversight regimes, for example, the Australian Federal Police is subject to oversight by the Commonwealth Ombudsman.

413. The use of force against a person by a constable or a staff member of the authorised agency is expressly ruled out as being authorised under this regime. This however would not exclude a police officer using force to arrest a person, under powers derived from other Commonwealth laws, who is obstructing a Commonwealth official in the performance of their functions (an offence under section 149.1 of the Criminal Code).

414. The chief executive of the authorised agency, staff members of the agency and constables assisting are not liable to an action or other proceeding (whether civil or criminal) for, or in relation to, an act or matter in good faith done or omitted to be done in the exercise, or purported exercise, of any power or authority conferred under this regime. This will ensure that the authorised agency is immune from civil or criminal liabilities when undertaking authorised actions at the request of the Secretary of Home Affairs.

415. In further support of effective oversight, the chief executive of the authorised agency is required to prepare a post-activity report as soon as possible able doing an act or thing in compliance with a request, but no later than 3 months. This report is to be provided to the Minister for Home Affairs and Defence Minister to ensure they have visibility of the actions that were taken and how they contributed to an effective response. This will assist the Government in monitoring the use of these powers, but also support future decision making in similar circumstances.

Hypothetical scenario:

A cyber security incident has rendered the computer network which supports a major metropolitan critical hospital inaccessible, resulting in the inoperability of all of the hospital wards including the general intensive care unit. The responsible entity of the critical hospital, and the managed service provider of the computer program which is central to the compromise, lack the technical expertise to patch the software to address the vulnerability and allow the entities to commence restoring services.

The Minister for Home Affairs is satisfied that patching the software is reasonable necessary and a proportionate response to the incident, is technically feasible and an action of a kind described by paragraph 35AC(f). The Minister for Home Affairs is also satisfied that the specific action that the entity is not technically capable of doing the action, and therefore directing them to do so would be futile. Having received the agreement of the Prime Minister and the Minister for Defence, the Minister authorises the Secretary requesting the assistance of the authorised agency to undertake the software patch.

Review of decisions made under Part 3A

416. The Bill inserts new paragraph (dae) into Schedule 1 of the *Administrative Decisions (Judicial Review) Act 1977* (ADJR Act) to include decisions under new Part 3A of the SOCI Act as decisions to which the ADJR Act does not apply.

417. This means judicial review under the ADJR Act will not be available for decisions made under new Part 3A of the SOCI Act.

418. The Administrative Review Council (ARC), in their 2012 report *Federal Judicial Review in Australia*, have identified a number of reasons that may justify an exemption from review under the ADJR Act. The ARC concluded that national security considerations may be a reason for excluding *ADJR Act* review, particularly where sensitive information is involved which may be publicly disseminated through judicial proceedings.

419. When making a decision under new Part 3A, the Minister for Home Affairs must be satisfied that a cyber security incident is sufficiently severe in relation to the social or economic stability of Australia or its people, the defence of Australia or national security. Decisions of this nature are likely to be based on sensitive classified information and deal with the capabilities of intelligence agencies. This includes intelligence information and covert investigation procedures, the disclosure of which may impact ongoing investigations or operations, or compromise intelligence methodologies. For this reason, it is entirely reasonable to exempt decisions made under new Part 3A from review under the ADJR Act as the public dissemination of the information and capabilities used to make decisions under new Part 3A would pose a risk to national security.

420. Similar to decisions made under the *Foreign Acquisitions and Takeovers Act 1975*, which are exempt from review under the ADJR Act, decisions made under new Part 3A will also deal with classified and commercially confidential material that is relevant to the operation of assets critical to Australia's economy. Owners and operators of critical infrastructure assets may be reluctant or unwilling to disclose such information to authorities for the purpose of new Part 3A if there is the

potential for this information to be disclosed in ADJR Act proceedings. This could delay or seriously inhibit the use of new Part 3A to protect assets critical to the economy. For this reason, it is appropriate for decisions dealing with such information to be exempt from the ADJR Act noting the potential impact to the economy if access to this information was undermined.

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

422. While exempt from review under the ADJR Act, new Part 3A includes certain safeguards and limitations to ensure that any decisions made by the Minister for Home Affairs to authorise the use of the mechanisms at sections 35AK, 35AQ or 35AX occur in exceptional circumstances and when it is in the national interest. Further, the original jurisdiction of the Federal Court and the High Court are unaffected.

ENFORCEMENT

423. Part 5 of the SOCI Act outlines the enforcement measures available to the Government if the civil penalty provisions within this Bill are contravened.

424. The Government's priority is to promote cooperative and collaborative working relationships with responsible entities and operators to encourage, and proportionately manage, risks associated with critical infrastructure assets. However, where there are instances of non-compliance with the obligations, the Bill establishes a range of enforcement options which can be scaled to address the particular circumstances of the non-compliance. For example, non-compliance which derives from a misunderstanding can be dealt with through closer engagement and education, while significant penalties could be pursued for repeated, serious violations by a non-cooperative entity.

425. The SOCI Act currently provides for the following suite of enforcement mechanisms through reliance on the Regulatory Powers (Standard Provisions) Act 2014 (Regulatory Powers Act):

- Seeking a civil penalty order from the relevant court for the person to pay the Government a pecuniary penalty in line with the civil penalty units assigned to the civil penalty provision;

- Enforceable undertaking allowing the Minister for Home Affairs or Secretary of Home Affairs to accept an undertaking relating to compliance with a civil penalty provision. Should the entity act contrary to the undertaking, the Minister or Secretary can seek an order from a relevant court to direct compliance with the undertaking, seek any financial benefit from the failure to comply with the undertaking to be surrendered, or seek an order for damages; and

- Injunctions, whether restraining a person from engaging in conduct that would be in contravention of a civil penalty provision, or a performance injunction to compel a person to comply with relevant obligations in the SOCI Act.

426. As the Bill inserts a broader range of obligations into the SOCI Act, the importance of a graduated enforcement scheme increases. An additional tool has been added through the activation of the powers to issue infringement notices under Part 5 of the Regulatory Powers Act. Part 5 of the Regulatory Powers Act provides standard provisions for an infringement notice framework which can be utilised where an officer reasonably believes that a provision of the Act has been contravened.

427. A person who is given an infringement notice can choose to pay an amount to dispose of the notice as an alternative to having court proceedings brought against the person to determine non-compliance. If the person does not choose to pay the amount, proceedings can be brought against the person in relation to the contravention. This allows for a less serious, and less administratively burdensome, alternative to seeking a court order and may be used as the first stage of a graduated to addressing non-compliance.

428. Further, the powers available to the Department of Home Affairs, or other relevant Commonwealth regulator, to effectively fulfil this regulatory role need enhancement to reflect the measures being introduced in the Bill. To supplement existing powers, primarily the Secretary's information gathering power in section 37 of the SOCI Act, the Bill will enliven the monitoring (Part 2) and investigation (Part 3) powers under the Regulatory Powers Act without modification. The intention in enlivening these Parts of the Regulatory Powers Act is to allow authorised persons, with the consent of the entity or under warrant, to:

- search premises, examine or observe any activity, inspect documents, operate electronic equipment and ask questions in order to determine whether an obligation under the Act is being complied with ('monitoring powers'); and

- search premises, inspect documents, seize evidence, operate electronic equipment and ask questions in order to gather evidence in relation to the contravention of an obligation under the Act ('investigation powers').

- As per the Regulatory Powers Act, a person who fails to answer a question from an authorised person, or to provide reasonable assistance and facilities to an authorised person and any person assisting the person, where premises have been entered under a warrant will be liable to a civil penalty.

429. These powers can be relied on to investigate compliance with civil penalty provisions in the SOCI as well as the offences in sections 35AT and 45 which relate to directions from the Secretary and unauthorised use or disclosure of protected information.

430. While this suite of powers and enforcement mechanisms will primarily be exercised by the Department of Home Affairs as the principle regulator of the regime, they also allow for a relevant Commonwealth regulator to exercise the powers. This will permit regulatory responsibility for obligations in relation to particular critical infrastructure assets to be exercised by another Commonwealth agency, should a more appropriate regulator be identified. Importantly, this option will prevent duplication in oversight of particular sectors and associated regulatory impost.

DIVISION 2 OF PART 6A —DECLARATION OF SYSTEMS OF NATIONAL SIGNIFICANCE BY THE MINISTER

431. Division 2 of Part 6A sets out the process by which the Minister for Home Affairs can declare a critical infrastructure asset to be a system of national significance. Systems of national significance are a smaller subset of critical infrastructure assets which are of the highest criticality due to their national significance. These are systems that are so integral to the functioning of modern society that their compromise, disruption or destruction would have significant adverse impacts on Australia's economic and social stability, defence and national security.

432. Systems of national significance are an attractive target for malicious actors, particularly those with the capability and motive to do significant harm to Australia's national interests. Due to these factors and the security vulnerabilities that may emerge if the extent of the assets criticality were widely known, a declaration under Part 6A is private, and the fact the declaration is made is protected information under the Act.

433. If an asset is declared by the Minister for Home Affairs to be a system of national significance, the Secretary is empowered to impose enhanced cyber security obligations contained in Part 2C on the entity in certain circumstances.

National significance

434. Subsection 52B(1) provides that the Minister for Home Affairs may declare a particular asset to be a system of national significance if the asset is a critical infrastructure asset and the Minister is satisfied that the asset is of national significance.

435. Subsection 52B(2) provides that, in determining whether an asset is of national significance, the Minister for Home Affairs must have regard to the nature and extent of interdependencies between the asset and other critical infrastructure assets that the Minister is aware of, as well as any other matters as the Minister considers relevant.

436. The systems that underpin our critical infrastructure are increasingly interconnected and digital. These interconnections, and convergence of informational technologies and operational technologies, provide economic benefits to owners and operators. System and process data can be drawn and leveraged to improve performance, identify faults and increase productivity. Internet-connected systems can be accessed from anywhere in the world, meaning that the unique skills required to rectify faults to these often aged assets can potentially be accessed whenever required. Critical infrastructure is also increasingly interdependent. Energy and communications underpin many other critical infrastructure sectors. Many assets in the communications sector provide a critical function which relies on electricity. Many critical infrastructure assets in turn rely on the communications sector to undertake their business.

437. However, this interconnectedness and interdependence creates a new set of vulnerabilities. Malicious actors can use these same digitally connected pathways to access, compromise, disrupt and destroy these critical systems. The compromise of one critical infrastructure asset could have first, second and third order consequences which cascade and compromise other critical infrastructure assets and critical infrastructure sectors.

438. The Minister for Home Affairs is not required to consider every interdependency between the asset and other critical infrastructure assets, however, may be satisfied of the national significance of the asset having considered a small number of interdependencies that are particularly significant or a large number of less significant, but nonetheless importance, dependencies.

Consultation with entities

439. Section 52C sets out the consultation requirements that must be undertaken prior to the Minister for Home Affairs making a declaration. Importantly, the Minister must provide the responsible entity of the asset with notice of the proposed declaration, including reasons for making the declaration, and invite any representations. The entity will ordinarily be provide 28 days to make any submissions, unless the Minister for Home Affairs is satisfied a shorter period is necessary due to urgent circumstances.

440. Noting that determining the criticality of an asset may rely on classified information, the Minister for Home Affairs is only required to provide reasons for the proposed declaration to the extent that it would not prejudice security.

SCHEDULE 2 – AMENDMENTS TO THE *CRIMINAL CODE*

441. This Schedule amends the *Criminal Code* in response to changes in technology, in particular the increasing prevalence of online, internet-based communications, which obscure the geographic location of parties to communications. The amendments update the Australian Signals Directorate's immunities to ensure it can continue to efficiently collect intelligence to protect

Australia's national security, foreign relations and national economic well-being, in an increasingly complex online environment.

442. The purpose of the amendments is to update the existing, limited immunities afforded to staff members and agents of the Australian Signals Directorate to ensure they remain effective in light of technological change. The underlying purpose of the immunities framework is to ensure that the staff members and agents of the Australian Signals Directorate are protected from civil and criminal liability for activities that are done in the proper performance of the Australian Signals Directorate's functions, including activities done to protect Australian critical infrastructure. These activities might otherwise be prohibited by Commonwealth, state or territory laws dealing with computer-related acts.

443. The Bill will remove Australian Signals Directorate from the existing immunities within section 476.5 and insert new section 476.6 into the *Criminal Code*. This amendment will provide limited immunities where an Australian Signals Directorate staff member or agent reasonably believes that the conduct is likely to cause a computer-related act, event, circumstance or result to take place outside Australia (whether or not it in fact takes place outside Australia). This amendment is required to allow ASD to continue to operate effectively in an increasingly challenging online environment, where it is not always possible to reliably determine the geographic location of a device or computer.

444. This challenge is exacerbated for the Australian Signals Directorate where adversaries (including foreign intelligence services and terrorist organisations) undertake cyber activities that harm Australia's critical infrastructure. To effectively perform its functions, and defend and respond to serious cyber incidents, the Australian Signals Directorate may need to engage in computer-related acts offshore, such as affecting the adversary's computer or device. However, where an adversary takes active steps to obfuscate their physical location, or where it is impossible for the Australian Signals Directorate to reliably determine their physical location, it is necessary to protect staff members and agents from liability if they inadvertently affect a computer or device located inside Australia.

445. The amendment will not provide staff members or agents of the Australian Signals Directorate with immunity from liability in circumstances where they know or believe an adversary's computer or device to be located in Australia. Nor will it provide such persons with immunity where their belief that an adversary's computer or device is located outside Australia is not reasonable. Consistent with current subsection 476.5(1), the immunity will continue to apply only where a staff member's or agent's conduct is done in the proper performance of an Australian Signals Directorate function.